UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

Nélida Maria Lima Brito da Graça Morais

Estudo sobre o grau de imperfeição em sub-reticulados do reticulado inteiro

Campinas-SP

2015

Nélida Maria Lima Brito da Graça Morais

Estudo sobre o grau de imperfeição em sub-reticulados do reticulado inteiro

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de mestra em Matemática Aplicada e Computacional.

Orientador: *Prof. Dr. João E. Strapasson*

O arquivo digital corresponde à versão final da dissertação defendida pela aluna Nélida Maria Lima Brito da Graça Morais e orientada pelo prof. Dr. João Eloir Strapasson

Assinatura do orientador

Campinas-SP

2015

Agência(s) de fomento e nº(s) de processo(s): Não se aplica.

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

M792e

Morais, Nélida Maria Lima Brito da Graça, 1981-
Estudo sobre o grau de imperfeição em sub-reticulados do reticulado inteiro / Nélida Maria Lima Brito da Graça Morais. – Campinas, SP : [s.n.], 2015.

Orientador: João Eloir Strapasson.
Dissertação (mestrado profissional) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Teoria dos reticulados. 2. Códigos quase-perfeitos. I. Strapasson, João Eloir,1979-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Study of imperfection degree in sub-lattices of the integer lattice
Palavras-chave em inglês:
Lattice theory
Quasi-perfect codes
Área de concentração: Matemática Aplicada e Computacional
Titulação: Mestra em Matemática Aplicada e Computacional
Banca examinadora:
João Eloir Strapasson [Orientador]
Grasiele Cristiane Jorge
Washington Alves de Oliveira
Data de defesa: 08-10-2015
Programa de Pós-Graduação: Matemática Aplicada e Computacional

Dissertação de Mestrado Profissional defendida em 08 de outubro de 2015

e aprovada pela Banca Examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). JOÃO ELOIR STRAPASSON

Prof(a). Dr(a). GRASIELE CRISTIANE JORGE

Prof(a). Dr(a). WASHINGTON ALVES DE OLIVEIRA

A Ata da defesa com as respectivas assinaturas dos membros
encontra-se no processo de vida acadêmica do aluno.

Ao Deus Todo-Poderoso. A Ti toda honra e toda glória.

Agradecimentos

Quero agradecer primeiramente à Deus, o autor da vida. Se não fosse por ele o que seria de mim? Meu amparo nas horas difíceis. Nos momentos que pensei que não conseguiria a sua palavra me dizia: “não te mandei Eu? Esforça te e tem bom ânimo”. A Ele minha gratidão e meu amor.

Deixo também outros agradecimentos importantes:

À minha família, Oziel e Jonathan, obrigada pelo suporte e pelo amor - amo muito voces!

Um muito obrigada aos meus pais e irmãos que sempre torceram por mim e pelo meu sucesso.

Ao meu orientador, João Strapasson - professor, quero um dia poder ter 1% da tua inteligência. Obrigada pela ajuda, sem você nada disso seria real - você é “o cara”.

Ao professor Cristiano pelo apoio e incentivo, meu muito obrigado.

À Igreja do Nazareno Memorial, representado pelo Pr. Silvano, que sempre nos apoiou e abençoou.

À família Oliveira (Adriane e Edson) que muitas vezes cuidou do meu filho para que eu pudesse frequentar as aulas. Vocês são especiais.

À FNB e ao Pr. Geraldo que facilitaram a minha chegada ao Brasil e me deram a possibilidade de começar esse sonho através do custeio da minha graduação. Minha eterna gratidão.

Aos meus colegas do mestrado, especialmente Gracielle, Paulo, Nazime e Marco pela camaradagem, pelas risadas e por cada momento que passamos juntos.

Por fim, mas não menos importante, a todos os meus amigos e irmãos da Igreja do Nazareno Memorial. Muito obrigada pelo suporte espiritual.

Resumo

Um dos grandes problemas em aberto na matemática até os dias de hoje é a questão do empacotamento esférico. Para tentar resolver este problema, tem-se estudado alguns fatores importantes inerentes a isso. Nesse trabalho apresentamos uma breve introdução à teoria de reticulados e teoria de códigos, onde trataremos conceitos como densidade de empacotamento e de cobertura.

O objetivo deste trabalho é o estudo da densidade de empacotamento e de cobertura em reticulados relativos à norma p. Neste estudo enfatizaremos o artigo "Quasi-perfect codes in the l_p metric" de Strapasson et al. [13] onde é estabelecida a noção de perfeição e imperfeição de reticulados relativos à norma p, e é apresentado um algoritmo que busca por reticulados perfeitos e quase-perfeitos.

Abstract

One of the major unsolved problems in Mathematics until the present day is the sphere packing issue. To try addressing this problem, some key factors related to this issue have been studied. We present a brief introduction to lattice theory and coding theory in the present paper in which we deal with concepts such as packing and covering densities.

The aim of the present work is the study of packing and covering densities on lattices related to p-metric. On this study we will highlight the article "Quasi-perfect codes in the l_p metric" from Strapasson et al. [13] where the concept of perfection and imperfection of lattices related to p-metric is established, and an algorithm which seeks perfect and quasi-perfect lattices is presented.

Sumário

1 Introdução **10**

2 Reticulados **11**

2.1 Alguns conceitos importântes em Reticulados 11

2.2 Alguns reticulados importantes 20

2.3 Redução de bases na dimensão 2 26

2.4 Problema do vetor mais curto e do vetor mais próximo 29

3 Códigos **33**

3.1 Códigos corretores de erros 33

3.2 Métrica de Hamming 34

3.3 Métrica de Lee 35

3.4 Códigos Perfeitos e quase-perfeitos na métrica de Lee 35

3.5 Métrica p-Lee 36

4 Grau de imperfeição **40**

4.1 Grau de Imperfeição 40

4.2 Lista de reticulados quase-perfeitos 43

Capítulo 1

Introdução

O objetivo desse trabalho foi de produzir um texto didático sobre a introdução ao estudo de reticulados e de códigos dando ênfase na busca por reticulados perfeitos e quase-perfeitos na norma p e trazendo o conceito de grau de perfeição. Este último conceito foi introduzido por Strapasson et al. [13].

O Capítulo 1 traz a introdução.

O Capítulo 2 é dedicado à introdução da teoria de reticulados e empacotamento reticulado. Neste capítulo definimos conceitos importantes como raios de empacotamento e cobertura, densidades de empacotamento, de centro e de cobertura, região fundamental e região de Voronoi. Também são apresentados os reticulados raízes e alguns dos melhores reticulados em termos de densidade de empacotamento e de cobertura. Aproveitamos para explanar um pouco sobre as formas de redução de bases, trazendo algoritmos para as reduções de Gauss, LLL e de Minkowski. Falamos brevemente dos problemas de encontrar o vetor mais curto (SVP) e o mais próximo (CVP). Referente ao SVP em um reticulado apresentamos o algoritmo proposto por Fincke and Pohst [4].

No Capítulo 3 o assunto principal é a teoria de códigos. Começa-se trazendo o conceito de códigos corretores de erros. Posteriormente apresentamos a métrica de Hamming, de Lee e a extensão dela chamada de métrica p-Lee. Trazemos um pouco sobre os conceitos de códigos perfeitos e quase-perfeitos na métrica l_p.

No quarto e último Capítulo trazemos o conceito de grau de imperfeição introduzido por Strapasson et al. [13]. Em tal artigo é introduzido o algoritmo apresentado aqui, que busca reticulados perfeitos e quase-perfeitos e ainda mostra o grau de imperfeição daqueles que não são perfeitos.

Capítulo 2

Reticulados

Um dos grandes problemas em aberto na matemática até os dias de hoje é a questão do empacotamento esférico. Esse problema visa saber qual o maior número de esferas idênticas que podemos empacotar deixando o menor espaço vazio possível. Quando os pontos onde se localizam os centros das esferas formam um grupo aditivo, chamamos esse empacotamento de empacotamento reticulado. As referências para este capítulo são Gouveia [6], Naves [10], Strapasson [12], Conway and Sloane [3], Strapasson et al. [13]

2.1 Alguns conceitos importântes em Reticulados

Definição 2.1. *Um* ***reticulado*** Λ *é definido como o conjunto de todas as combinações inteiras de n vetores linearmente independentes* β=$\{v_1, v_2, ..., v_m\}$ *com* $v_i \in \mathbb{R}^n$ *. Isto é,*

$$\Lambda = \left\{ \sum_{i=1}^{m} x_i v_i | x_i \in \mathbb{Z} \right\}$$

O conjunto $\beta = \{v_1, v_2, ..., v_n\}$ é chamado de **base** do reticulado.

Exemplo 2.2. A figura 2.1 ilustra um reticulado Λ cuja base β é dada por $\beta = \left\{ \left(\frac{2}{5}, 1\right), \left(\frac{8}{5}, -\frac{6}{5}\right) \right\}$.

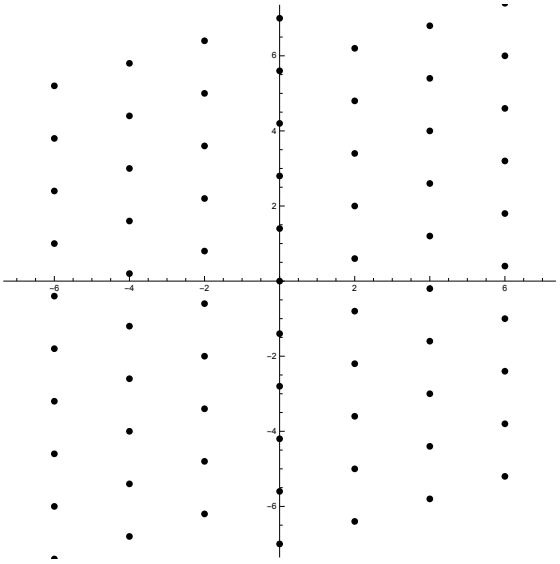

Figura 2.1: Exemplo de Reticulado gerado pela base $\left\{\left(\frac{2}{5},1\right),\left(\frac{8}{5},-\frac{6}{5}\right)\right\}$

Tomando os vetores da base como linha, formamos uma matriz B denominada **matriz geradora**, dada por:

$$B = \begin{bmatrix} v_{11} & \dots & v_{n1} \\ \vdots & \ddots & \vdots \\ v_{1n} & \dots & v_{nn} \end{bmatrix}$$

No Exemplo 2.1 a matriz geradora é dada por

$$B = \begin{bmatrix} \frac{2}{5} & 1 \\ \frac{8}{5} & -\frac{6}{5} \end{bmatrix}$$

Frisamos que a base de um reticulado não é única. Duas matrizes B e B' geram o mesmo reticulado Λ, se e somente se, existir uma matriz U unimodular, isto é, com coordenadas inteiras e determinante igual a ± 1, tal que $B' = UB$.

Exemplo 2.3. Consideremos uma matriz geradora B de um reticulado Λ e U uma matriz unimodular, onde $B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ e $U = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$, então

$$B' = UB = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} . \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$$

também gera Λ.

Note que de fato a base $\{(0,1),(1,0)\}$ pode ser escrita como combinação linear de

$\beta' = \{(2,1),(1,1)\}$, isto é:

$$(0,1) = x(2,1) + y(1,1) \iff \begin{cases} 2x + y = 0 \\ x + y = 1 \end{cases} \Rightarrow x = -1,\ y = 2$$

$$(1,0) = x(2,1) + y(1,1) \iff \begin{cases} 2x + y = 1 \\ x + y = 0 \end{cases} \Rightarrow x = 1,\ y = -1$$

Pode-se notar também que a matriz formada por x e y $\begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}$ é exatamente a inversa de U.

Definição 2.4. *Sendo B a matriz geradora do reticulado Λ, definimos a* ***matriz de Gram*** *como*

$$G = BB^t$$

onde B^t é a transposta de B.

Exemplo 2.5. No exemplo 2.3 a matriz de Gram é dada por

$$G = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} . \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Se considerarmos B' que gera o mesmo reticulado temos a sua matriz de Gram dada por

$$G' = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} . \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix}$$

Exemplo 2.6. Dado uma matriz geradora $C = \begin{bmatrix} 2 & -1 \\ 1 & 3 \end{bmatrix}$, a sua matriz de Gram, G será dada por

$$G = C^t C = \begin{bmatrix} 2 & 1 \\ -1 & 3 \end{bmatrix} . \begin{bmatrix} 2 & -1 \\ 1 & 3 \end{bmatrix} = \begin{bmatrix} 5 & 1 \\ 1 & 10 \end{bmatrix}$$

O **determinante** de um reticulado Λ ($det(\Lambda)$) é dado pelo determinante da sua matriz de Gram, ou seja, $det(\Lambda) = det(G)$

Como a base de um reticulado não é única, a matriz de Gram também não é, porém o seu determinante continua sendo o mesmo.

Considerando duas matrizes geradoras$B$ e B' de um reticulado Λ, onde G e G' representam as matrizes de Gram relacionadas a B e B', temos que

$$det(G) = det(G')$$

De fato, temos que existe U unimodular tal que $B' = UB$ e daí,

$$det\left(G'\right) = det\left(B'B''^{t}\right) = det\left(UBB^{t}U^{t}\right) = \underbrace{det\left(U\right)}_{\pm 1} det\left(BB^{t}\right) \underbrace{det\left(U^{t}\right)}_{\pm 1}$$

$$= det\left(BB^{t}\right) = det\left(G\right) \Longleftrightarrow det\left(G'\right) = det\left(G\right)$$

Exemplo 2.7. Considere as bases $\beta = \{(1,0),(0,1)\}$ e $\beta' = \{(2,1),(1,1)\}$, e as respectivas matrizes de Gram

$$G = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \; e \; G' = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} . \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix}$$

$$det\left(G\right) = det\left(G'\right) = 1$$

Ao fazermos uma rotação, translação ou mudança de escala de um certo reticulado, obtemos outro reticulado dito **equivalente** ao primeiro.

Definição 2.8. *Dois reticulados $\Lambda_1 e\, \Lambda_2$ são **equivalentes** se e somente se, as suas respectivas matrizes geradoras B e B' se relacionarem da seguinte forma:*

$$B' = cUBA$$

onde $c \in \mathbb{R}$ e $c > 0$, U é uma matriz unimodular (coordenadas inteiras e determinante igual a ± 1) e A uma matriz ortogonal, isto é, $AA^{t} = I$.

Suas matrizes de Gram G e G' respectivamente, se relacionam da seguinte forma:

$$G' = c^{2}UGU^{t}$$

Caso $c = 1$, os reticulados são ditos **congruentes**.

Consideremos $X = (x_1, x_2, ..., x_n)$ pertencente ao reticulado Λ, a norma de X é dada por,

$$\|X\| = \sqrt{\langle X, X\rangle} = \sqrt{\sum_{i=1}^{n} x_i^2}$$

Definição 2.9. *Chamamos de **norma mínima** ou **distância mínima** de um reticulado a menor distância entre dois pontos distintos de um reticulado, isto é,*

$$d = min\left\{\|X\| \mid X \in \Lambda \, e \, X \neq 0\right\}.$$

*Os vetores que realizam a distância mínima serão chamados de **vetores mínimos**.*

Definição 2.10. *Considere $\mathcal{F}$ um conjunto fechado e não nulo apoiado na base do reticulado. Este conjunto é chamado de **paralelepípedo fundamental** ou **região funda-***

mental *do reticulado* Λ*, isto é,*

$$\mathcal{F} = \sum_{i=1}^{n} a_i v_i \ com\ 0 \leq a_i \leq 1.$$

A união das translações da região fundamental em pontos do reticulado cobre todo o plano.

Definição 2.11. *Considere um reticulado* Λ*, a sua base* β*, e* V *um subespaço vetorial do* $\mathbb{R}^n$ *gerado por* β*. Considere também um ponto* v *pertencente a* V*, a região de Voronoi de* v *(*$vor\,(v)$*) é o conjunto dos pontos de* V *que estão mais próximos de* v *do que qualquer outro ponto* u*, isto é,*

$$vor\,(v) = \{x \in V : dist\,(x, v) \leq dist\,(x, u)\,, \forall u \in \Lambda\}$$

A região de Voronoi é uma região fundamental de Λ*. Ressaltamos que o volume de qualquer região fundamental é sempre o mesmo.*

Exemplo 2.12. A figura 2.2 ilustra a região de Voronoi de um reticulado Λ.

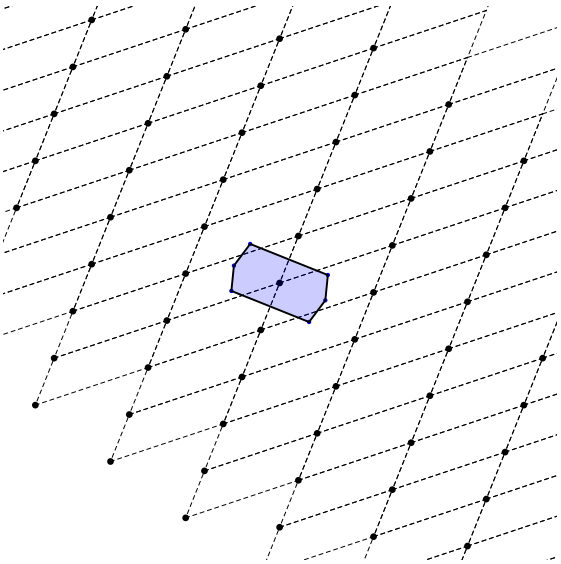

Figura 2.2: Região de Voronoi

Se considerarmos as regiões de Voronoi dos pontos de um reticulado poderemos verificar que os seus interiores são regiões disjuntas, porém compartilham dois a dois de uma mesma face.

O conjunto das regiões de Voronoi de todos os pontos pertencentes ao reticulado Λ forma um ladrilhamento perfeito no plano. Tendo por exemplo a região de Voronoi da origem ($vor\,(0)$) podemos obter todas as outras fazendo uma translação desta, isto é,

$$vor\,(v) = v + vor\,(0)\,,\ \forall v \in \Lambda$$

Exemplo 2.13. Ladrilhamento por região de Voronoi e a região fundamental (a menor com base reduzida)

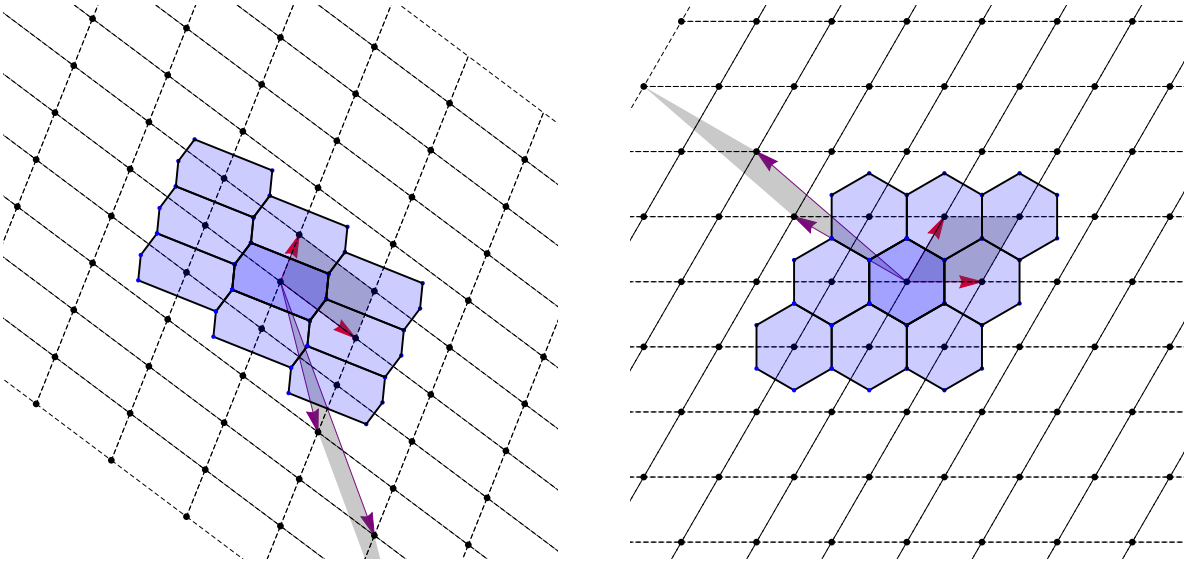

Figura 2.3: Reticulado, Região de Voronoi e Região Fundamental

Definição 2.14. *Qualquer reticulado n- dimensional Λ_n possui um reticulado dual (Λ_n^*), definido por*

$$\Lambda_n^* = \{x \in \mathbb{R}^n : \langle x, u\rangle \in \mathbb{Z}, \forall u \in \Lambda_n\}$$

Considerando um reticulado Λ_n com matriz geradora B e matriz de Gram G, então o seu dual Λ_n^* possui matriz de Gram dada por G^{-1} e portanto o seu determinante é

$$det\left(\Lambda_n^*\right) = det\left(G^{-1}\right) = \frac{1}{det\left(G\right)} = \left(detG\right)^{-1} = det\left(\Lambda_n\right)^{-1}$$

$$\therefore det\left(\Lambda_n^*\right) = det\left(\Lambda_n\right)^{-1}$$

A matriz geradora de Λ_n^* é dada por $\left(B^{-1}\right)^t$.

2.1.1 Empacotamento esférico

O problema de empacotamento esférico é um dos grandes problemas até hoje sem solução. Empacotar esferas significa saber a melhor forma de dispor esferas de mesmo raio num determinado espaço, onde as esferas podem se tocar apenas nos bordos. O empacotamento perfeito seria aquele onde o espaço seria ocupado na totalidade (ou é deixado o mínimo de espaço entre as esferas). No nosso caso estaremos dando ênfase ao empacotamento reticulado.

Definição 2.15. *Empacotamento reticulado, é o tipo de empacotamento esférico onde o centro das esferas é um reticulado.*

Exemplo 2.16. A figura 2.4 nos mostra alguns exemplos de empacotameno reticulado.

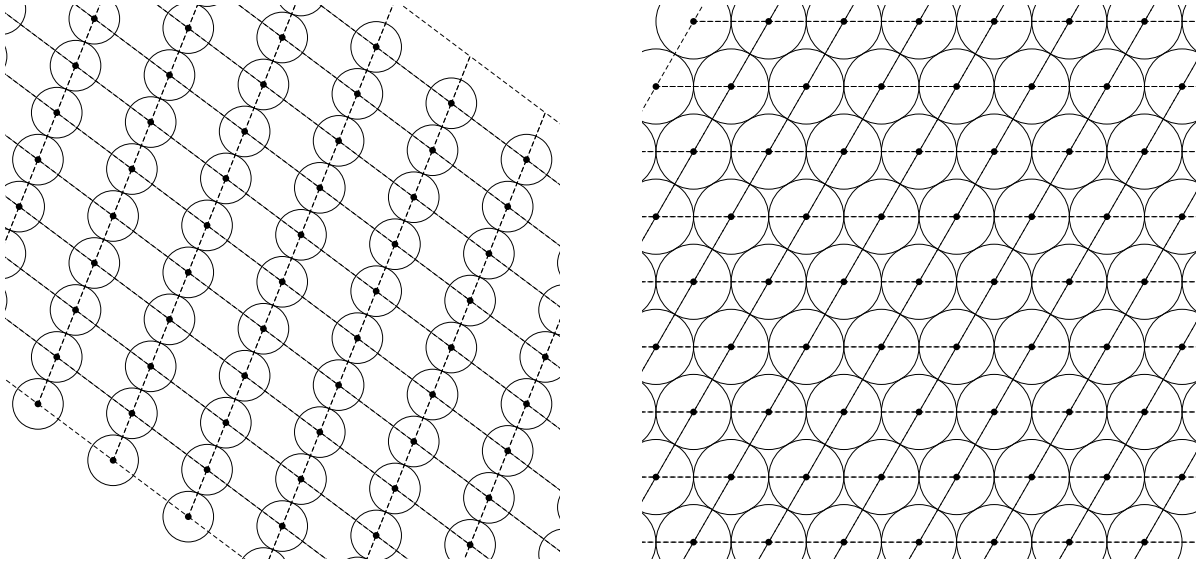

Figura 2.4: Empacotamentos gerados pelos reticulados $\left\{\left(-\frac{7}{5},\frac{2}{5}\right),(0,2)\right\}$ e $\left\{(1,0),\left(\frac{1}{2},\frac{\sqrt{3}}{2}\right)\right\}$ respectivamente

Em muitos casos o melhor empacotamento é o reticulado.

Definição 2.17. *O* ***raio de empacotamento*** *é o maior raio de um dado empacotamento, isto é, dado duas bolas abertas de raio r centradas em u e v, com u e v pertencentes ao reticulado e u diferente de v, temos que,*

$$B_r(u) \cap B_r(v) = \phi$$

Ou em outras palavras, é o maior raio que podemos usar para que as nossas bolas não tenham ponto em comum no interior, embora essas bolas possam se tocar no bordo. O raio de empacotamento é a metade da distância mínima entre dois pontos do reticulado.

Exemplo 2.18. Considerando o reticulado $\mathbb{Z}^2$, que é um reticulado gerado pela base canônica do $\mathbb{R}^2$. Temos que seu raio de empacotamento é $1/2$.

Densidade de empacotamento, Δ, é a proporção do espaço ocupado pelas esferas.

$$\Delta = \frac{volume\,de\,uma\,esfera\,de\,empacotamento}{volume\,da\,região\,fundamental}$$

O volume da região funtamental por sua vez, é dado por $(\det\Lambda)^{\frac{1}{2}}$, logo a densidade de empacotamento é dada por

$$\Delta = \frac{volume\,uma\,esfera}{(det\Lambda)^{1/2}} \tag{2.1}$$

Em dimensões maiores que 3 precisamos saber o volume da esfera n-dimensional de raio r, dado por

$$V_n r^n \tag{2.2}$$

onde V_n é o volume da esfera de raio 1 e é dado por

$$V_n = \frac{\pi^{n/2}}{(n/2)!} = \frac{2^n \pi^{\frac{n-1}{2}} \frac{n-1}{2}!}{n!}$$

Relacionando 2.1 e 2.2, temos que, a densidade de empacotamento reticulado é dado por

$$\Delta = \frac{V_n r^n}{(det\Lambda)^{1/2}} \tag{2.3}$$

A densidade de empacotamento nos mostra a qualidade do nosso empacotamento, quanto mais próximo de 1 melhor será o empacotamento. Por exemplo, na dimensão 2 o reticulado mais denso é o reticulado hexagonal, gerado por $\left\{(1,0), \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)\right\}$, cuja densidade de empacotamento é $\Delta \simeq 0,9069$. Já na dimensão 3, o reticulado mais denso, encontrado até hoje é o fcc (face-centred cubic) que é um reticulado gerado pela base $\{(1,0,1), (0,1,1), (1,1,0)\}$ e cuja densidade vale $\Delta \simeq 0,74048$.

Proposição 2.19. *Reticulados equivalentes têm a mesma densidade de empacotamento.*

Demonstração. Sejam dois reticulados equivalentes Λ e Λ' com as respectivas densidades de empacotamento dadas por Δ e Δ' e matrizes de Gram dadas por G e G'.

Seja Δ' dada por $\Delta' = \frac{V_n r'^n}{(det\Lambda')^{1/2}} = \frac{V_n r'^n}{(detG')^{1/2}}$.

Como os reticulados são equivalentes, os seus raios e suas matrizes de Gram se relacionam através de uma constante k, isto é, $r' = kr$ e $G' = kG$.

Portanto,

$$\Delta' = \frac{V_n r'^n}{(det\Lambda')^{1/2}} = \frac{V_n r'^n}{(detG')^{1/2}} = \frac{V_n k^n r^n}{k^n det\,(G)} = \frac{V_n r^n}{det\,(G)} = \Delta$$

□

Definição 2.20. *Dado uma esfera de raio $r = 1$, a **densidade de centro** (δ) é dada por*

$$\delta = \frac{\Delta}{V_n}$$

Tomando o valor de Δ em 2.3 , temos então que, no empacotamento reticulado a densidade de centro pode ser dada por

$$\delta = \frac{r^n}{(det\Lambda)^{1/2}}$$

A tabela 2.1 nos mostra alguns valores da densidade de empacotamento e de centro de alguns reticulados. Por exemplo, na dimensão 1 temos o reticulado A_1 que pertence à família dos reticulados n-dimensionais chamados de reticulados raizes A_n(neste caso $n = 1$) com densidade de empacotamento Δ igual a 1 e densidade de centro δ igual a $0,5$. Na dimensão 2 temos o reticulado A_2 (A_n, com $n = 2$) que é equivalente ao reticulado *hexagonal* e tem densidade de empacotamento Δ igual a $0,90690$ e densidade de centro δ igual a $0,28868$. Os reticulados A_1, A_2, D_3, D_4, D_5, E_6, E_7 e E_8 serão estudados nas subsecções 2.2.2, 2.2.3 e 2.2.4. A tabela foi extraída de Conway and Sloane [3].

Tabela 2.1: Densidade de empacotamento e de centro

Dimensão (n)	Nome do empacotamento	Densidade (Δ)	Densidade de centro (δ)
1	A_1	1	0,5
2	A_2	0,90690	0,28868
3	D_3	0,74048	0,1847
4	D_4	0,61685	0,13127
5	D_5	0,46526	0,09987
6	E_6	0,37295	0,08112
7	E_7	0,29530	0,06981
8	E_8	0,25367	0,06326

Tudo o que temos visto até agora tem a ver com o *problema de empacotamento*, mas outro problema em reticulados é o *problema de cobertura* que pode ser considerado como o *dual* do problema de empacotamento. O problema de cobertura busca a forma mais econômica de cobrir um espaço n-dimensional com esferas sobrepostas.

Definição 2.21. *O* ***raio de cobertura*** *, R, é dado pelo raio da menor esfera que circunscreve a sua região de Voronoi.*

A ***densidade de cobertura*** *(Θ) é dado por*

$$\Theta = \frac{volume\ de\ uma\ esfera\ de\ cobertura}{(det\Lambda)^{1/2}} = \frac{V_n R^n}{(det\Lambda)^{1/2}}$$

Ou seja, a densidade de cobertura é dada pela razão entre o volume de uma esfera com raio de cobertura R e o volume do reticulado.

A densidade de cobertura é definida de forma semelhante à densidade de empacotamento, salvo que o raio utilizado é o de cobertura R.

Enquanto que a densidade de empacotamento Δ é sempre menor ou igual a 1, a densidade de cobertura Θ é sempre maior ou igual a 1.

$$\Delta \leq 1 \leq \Theta$$

Definição 2.22. *O problema de cobertura busca por um valor mínimo de densidade de cobertura.*

A tabela 2.2 nos mostra o valor da densidade de cobertura de alguns reticulados nas dimensões de 1 ao 8. Por exemplo na dimensão 1 a cobertura feita pelo reticulado A_1^*, que é o dual do reticulado A_1, é equivalente ao reticulado $\mathbb{Z}$, reticulado inteiro (secção 2.2.1) na dimensão 1 , e tem a densidade de cobertura igual a 1. Os reticulados A_n^* e D_n^* são os duais dos reticulados A_n e D_n respectivamente, e serão estudados nas secções 2.2.2 e 2.2.3.

Dimensão (n)	Nome da Cobertura	Densidade de cobertura (Θ)
1	$A_1^* \cong \mathbb{Z}$	1
2	$A_2^* \cong A_2$	1,2092
3	$A_3^* \cong D_3^*$	1,4635
	$A_3 \cong D_3$	2,0944
4	A_4^*	1,7655
	$D_4^* \cong D_4$	2,4674
	A_4	3,1780
5	A_5^*	2,1243
	D_5^*	2,4982
6	A_6^*	2,5511
	D_6^*	4,3603
7	A_7^*	3,0596
	E_7^*	4,1872
	D_7^*	4,5687
8	A_8^*	3,6658
	E_8	4,0587
	D_8^*	8,1174

Tabela 2.2: Valor da densidade de cobertura em alguns reticulados

Na tabela 2.3 listamos alguns dos melhores reticulados, até a dimensão 8, em termos de empacotamento mais denso e de melhor cobertura. Por exemplo, na dimensão 2 o empacotamento mais denso e a melhor cobertura é oferecida pelo reticulado A_2. A tabela é baseada no livro Conway and Sloane [3]

Dimensão	1	2	3	4	5	6	7	8
Empacotamento mais denso	$\mathbb{Z}$	A_2	A_3	D_4	D_5	E_6	E_7	E_8
Melhor cobertura	$\mathbb{Z}$	A_2	A_3^*	A_4^*	A_5^*	A_6^*	A_7^*	A_8^*

Tabela 2.3: Melhores reticulados até dimensão 8

2.2 Alguns reticulados importantes

Nesta secção serão apresentados alguns reticulados importantes e algumas das suas características, como matriz geradora, norma mínima, vetor mínimo, raios de empacotamento e cobertura e densidades de empacotamento, centro e cobertura.

A referência para essa secção é Conway and Sloane [3].

2.2.1 Reticulado $\mathbb{Z}^n$

$\mathbb{Z}$ é o conjunto dos números inteiros, i.e., $\mathbb{Z} = \{\ldots - 2, -1, 0, 1, 2, \ldots\}$.

$\mathbb{Z}^n = \{(x_1, \ldots, x_n) : x_i \in \mathbb{Z}\}$ é o reticulado n-dimensional ou reticulado inteiro.

Uma possível e mais simples matriz geradora para o $\mathbb{Z}^n$ é a matriz identidade. Baseado nisso, será mostrado algumas características (informações) importantes referentes a esse tipo de reticulado.

- O determinante de $\mathbb{Z}^n$, $det\,(\mathbb{Z}^n) = 1$.
- A sua norma mínima é igual a 1.
- Os vetores mínimos são $(0, \ldots, \pm 1, \ldots, 0)$.
- O seu raio de empacotamento, r, é dado por $r = \frac{1}{2}$.
- O raio de cobertura, R, é dado por $R = r\sqrt{n} = \frac{\sqrt{n}}{2}$.
- A densidade de cobertura é $\Delta = V_n 2^{-n}$ ($\Delta_{\mathbb{Z}} = 1$, $\Delta_{\mathbb{Z}^2} = \pi/4 = 0,785$, $\Delta_{\mathbb{Z}^3} = \frac{\pi}{6} = 0,524$, $\Delta_{\mathbb{Z}^4} = \frac{\pi^2}{32} = 0,308$).
- A densidade de centro é $\delta = 2^{-n}$
- As suas regiões de Voronoi são cubos.

Os reticulados $\mathbb{Z}^n$ são os duais deles mesmos.

2.2.2 Reticulados A_n e A_n^*

Um reticulado A_n, para $n \geq 1$, é dado por

$$A_n = \left\{ (x_0, x_1, \ldots, x_n) \in \mathbb{Z}^{n+1}, \sum_{i=0}^{n} x_i = 0 \right\}$$

Nota-se que para definirmos um reticulado n-dimensional $A_n \subset \mathbb{R}^m$ com $m > n$ precisamos de $n + 1$ coordenadas.

Exemplo 2.23. O reticulado A_2 é gerado pela base $\{(1, -1, 0), (0, 1, -1)\}$.

Uma matriz geradora para A_n é dada por

$$B = \begin{bmatrix} 1 & -1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & -1 & 0 & \ldots & 0 & 0 \\ 0 & 0 & 1 & -1 & \ldots & 0 & 0 \\ 0 & 0 & 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \ldots & -1 & 0 \\ 0 & 0 & 0 & 0 & \ldots & 1 & -1 \end{bmatrix}$$

E uma matriz de Gram é

$$G = \begin{bmatrix} 2 & -1 & 0 & \dots & 0 & 0 \\ -1 & 2 & -1 & \dots & 0 & 0 \\ 0 & -1 & 2 & \dots & 0 & 0 \\ \dots & \dots & \dots & \ddots & \dots & \dots \\ 0 & 0 & 0 & \dots & 2 & -1 \\ 0 & 0 & 0 & \dots & -1 & 2 \end{bmatrix}$$

Passaremos então a algumas características de um reticulado A_n.

- O determinante é $det\,(A_n) = n + 1$.
- A norma mínima é igual a 2.
- Os vetores mínimos são dados por qualquer permutação de $(1, -1, 0, \dots, 0)$.
- O raio de empacotamento é $r = \frac{1}{\sqrt{2}}$.
- A densidade de centro é dada por $\delta = 2^{-n/2}\,(n+1)^{-1/2}$.
- O raio de cobertura por sua vez é $R = r\left\{\frac{2a(n+1-a)}{n+1}\right\}^{1/2}$ onde a é a parte inteira de $\frac{n+1}{2}$.

Particularmente, temos que:

$A_1 \cong \mathbb{Z}$ e A_2 equivale ao reticulado Hexagonal. Uma matriz geradora para esse reticulado pode ser dada por

$$B = \begin{bmatrix} 1 & 0 \\ -\frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix}$$

Neste caso o determinante é $3/4$, a norma mínima é igual a 1 e os vetores mínimos são dados por $(\pm 1, 0)$ e $\left(\pm\frac{1}{2}, \pm\frac{\sqrt{3}}{2}\right)$. Os raios de empacotamento e cobertura são dados respectivamente por $r = 1/2$ e $R = \frac{2r}{\sqrt{3}}$. Por sua vez as densidades de empacotamento e de centro são $\Delta = \frac{\pi}{\sqrt{12}} = 0,9069$ e $\delta = \frac{1}{\sqrt{12}}$ respectivamente.

A_3(também o D_3) é equivalente ao reticulado fcc (face-centered cubic).

Uma matriz geradora para o reticulado fcc é

$$B = \begin{bmatrix} -1 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{bmatrix}$$

O determinante desse mesmo reticulado é $det\,(fcc) = 4$. A sua norma mínima é 2 e os vetores mínimos são dados pelas permutações de $(\pm 1, \pm 1, 0)$. Os raios de empacotamento

e cobertura são $r = \frac{1}{\sqrt{2}}$ e $R = r\sqrt{2} = 1$ respectivamente. A densidade de empacotamento e de centro são respectivamente $\Delta = \frac{\pi}{\sqrt{18}}$ e $\delta = 2^{-5/2}$. As regiões de Voronoi são dodecaedros rómbicos.

Quanto ao reticulado A_n^*, sabemos que é o dual do reticulado A_n e a sua matriz geradora é dada por

$$B = \begin{bmatrix} 1 & -1 & 0 & \dots & 0 & 0 \\ 1 & 0 & -1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 0 & 0 & \dots & -1 & 0 \\ -\frac{n}{n+1} & \frac{1}{n+1} & \frac{1}{n+1} & \cdots & \frac{1}{n+1} & \frac{1}{n+1} \end{bmatrix}$$

Por ser o dual do reticulado A_n, o determinante do reticulado A_n^* pode ser obtido da seguinte forma

$$det\,(A_n^*) = det\,(A_n)^{-1} = \frac{1}{n+1}.$$

A sua norma mínima é $\frac{n}{n+1}$, o raio de empacotamento é $r = \frac{1}{2}\sqrt{\frac{n}{n+1}}$, o raio de cobertura é $R = r\sqrt{\frac{n+2}{3}} = \sqrt{\frac{n(n+2)}{12(n+1)}}$, a densidade de centro e a densidade de cobertura são respectivamente $\delta = \frac{n^{n/2}}{2^n(n+1)^{(n-1)/2}}$ e $\Theta = V_n\sqrt{n+1}\left(\frac{n(n+2)}{12(n+1)}\right)^{n/2}$.

O reticulado A_1^* é equivalente aos reticulados A_1 e $\mathbb{Z}$, enquanto que o reticulado A_2^* se equivale a A_2. O reticulado A_n^* representa a melhor cobertura do $\mathbb{R}^n$ em várias dimensões como nos mostra a tabela 2.3. Já o A_3^*, assim como o D_3^* são equivalentes ao reticulado conhecido como o *body centered cubic (bcc),* que pode ser gerado pela seguinte matriz:

$$B = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

O determinante neste caso é igual a 16, a norma mínima é 3 e os vetores mínimos são todas as permutações de $(\pm 1, \pm 1, \pm 1)$. Já os raios de empacotamento e cobertura são respectivamente $r = \frac{\sqrt{3}}{2}$ e $R = \frac{\sqrt{5}}{2}$. As densidades de empacotamento, de centro e de cobertura são $\Delta = \frac{\pi\sqrt{3}}{8} = 0,6802$, $\delta = \frac{3\sqrt{3}}{32}$ e $\Theta = \pi\frac{5\sqrt{5}}{24} = 1,4635$. As regiões de Voronoi são tetraedros truncados.

2.2.3 Reticulados D_n e D_n^*

Definimos o reticulado D_n como:

$$D_n = \{(x_1, \dots, x_n) \in \mathbb{Z}^n \colon x_1 + \dots + x_n \quad \acute{e}\ par\}$$

Segundo Conway and Sloane [3], o reticulado D_n é obtido colorindo os pontos de $\mathbb{Z}^n$

alternadamente como num tabuleiro de damas, por esse motivo esse reticulado algumas vezes é chamado de *reticulado Checkerboard* (tabuleiro de damas). Uma matriz geradora é dada por

$$B = \begin{bmatrix} -1 & -1 & 0 & \dots & 0 & 0 \\ 1 & -1 & 0 & \dots & 0 & 0 \\ 0 & 1 & -1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & -1 \end{bmatrix}$$

O determinante do reticulado é 4, a norma mínima é 2, os vetores mínimos são todas as permutações de $(\pm 1, \pm 1, 0, \dots, 0)$, o raio de empacotamento é $r = \frac{1}{\sqrt{2}}$, o raio de cobertura é $R = r\sqrt{n}$ para $n = 3$ ou $r\sqrt{n/2}$ para $n \geq 4$ e a densidade de centro é $\delta = 2^{-(n+2)/2}$.

Particularmente temos que o reticulado D_3, assim como o A_3, é equivalente ao reticulado fcc mecionado anteriormente. O reticulado D_4 é equivalente ao reticulado dual D_4^*, os vetores mínimos são dadas pela permutação de $(\pm 1, \pm 1, 0, 0)$, o raio de cobertura é 1, a densidade de empacotamento é $\Delta = \frac{\pi^2}{16} = 0,6169$, a densidade de centro é $\delta = \frac{1}{8}$ e a densidade de cobertura é $\Theta = \frac{\pi^2}{4} = 2,4674$.

Quanto ao reticulado D_n^* sabe se que se trata do reticulado dual de D_n. Uma base para esse reticulado é dada por

$$B = \begin{bmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \dots & \frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

O seu determinante vale $\frac{1}{4}$, a norma mínima vale $\frac{3}{4}$ para $n = 3$ e 1 para $n \geq 4$, o raio de empacotamento vale $r = \frac{\sqrt{3}}{4}$ para $n = 3$ e $r = \frac{1}{2}$ para $n \geq 4$. A densidade de empacotamento é dada por $\delta = 3^{1,5}2^{-5}$ para $n = 3$ e $\delta = 2^{-(n-1)}$para $n \geq 4$. O raio de cobertura vale $R = r\sqrt{\frac{n}{2}}$ para n par, $R = r\sqrt{5/3}$ para $n = 3$ ou $\frac{r\sqrt{2n-1}}{2}$ para $n \geq 5$ e ímpar.

Como já foi dito anteriormente D_3^* é equivalente ao fcc e o D_4^* é equivalente ao D_4.

2.2.4 Reticulados E_6, E_7 e E_8

Começaremos pelo E_8 porque a definição de E_6 e E_7 advem dele.

- O reticulado E_8 pode ser definido como

$$E_8 = \left\{ x \in \mathbb{R}^8 : x_i \in \mathbb{Z} \; ou \; x_i \in \mathbb{Z} + \frac{1}{2}, \; \sum x_i \equiv 0 \; (mod 2) \right\}$$

Uma base para o E_8 é dada por

$$B = \begin{bmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

A norma mínima é 2, os vetores mínimos são dados pelas permutações de $(\pm 1^2, 0^6)$. O raio de empacotamento é $r = \frac{1}{\sqrt{2}}$ e o raio de cobertura é $R = r\sqrt{2} = 1$. Quanto as densidades de empacotamento e de centro, temos que $\Delta = \frac{\pi^4}{384} = 0,2537...$ e $\delta = \frac{1}{16}$. A densidade de cobertura é dada por $\Theta = \frac{\pi^4}{24} = 4,0587..$

- O reticulado E_7 é um subconjunto de E_8 que pode ser representado, por exemplo do seguinte modo:

$$E_7 = \{x \in E_8 : \ x.v = 0, \ v \in E_8\}$$

ou seja, o reticulado E_7 é composto pelos vetores pertencentes ao reticulado E_8 e que são perpendiculares a um vetor v de norma mínima pertencente a E_8. Uma base para o E_7 é dada por B,onde

$$B = \begin{bmatrix} -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

Neste caso o vetor mínimo é dado pelas permutações de $(-1, 1, 0, 0, 0, 0, 0, 0)$ ou de $\left(\left(\frac{1}{2}\right)^4, \left(-\frac{1}{2}\right)^4\right)$. A norma mínima é 2. Os raios de empacotamento e cobertura são respectivamente $r = \frac{\sqrt{2}}{2}$ e $R = r\sqrt{3} = \sqrt{\frac{3}{2}}$ e as densidades de empacotamento e centro são respectivamente $\Delta = \frac{\pi^3}{105} = 0,2953$ e $\delta = \frac{1}{16}$.

- Quanto ao reticulado E_6, podemos definí-lo da seguinte forma

$$E_6 = \{x \in E_8 : \ x.v = 0, \ \forall v \in V\}$$

onde V é um sub-reticulado de E_8. Um gerador para o E_6 é dado por

$$B = \begin{bmatrix} 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{bmatrix}$$

A norma mínima é 2, os vetores mínimos são dados pelas permutações do vetor $(0, 1, -1, 0, 0, 0, 0, 0)$. Os raios de empacotamento e de cobertura são $r = \frac{\sqrt{2}}{2}$ e $R = r\sqrt{\frac{8}{3}} = \frac{2\sqrt{3}}{3}$ respectivamente. E as densidades de empacotamento e de centro são respectivamente $\Delta = \frac{\pi^3}{48\sqrt{3}} \cong 0,379$ e $\delta = \frac{1}{8\sqrt{3}}$.

2.3 Redução de bases na dimensão 2

Reduzir bases significa encontrar uma base de um reticulado cujos vetores são os menores possíveis e o mais próximo possível de serem ortogonais.

Nesta secção falaremos resumidamente sobre o método de Gauss, o método LLL, que devemos a Lenstra, Lenstra e Lovász, e o método de redução de Minkowski.

As referência para esta secção são Strapasson [12], Galbraith [5], Campello [2], Conway and Sloane [3]

2.3.1 Redução de Gauss

Teorema 2.24. *Sejam λ_1 e λ_2 os mínimos sucessivos de Λ. Se Λ possuir uma base ordenada $\{v_1, v_2\}$ Gauss-reduzida, então $\|v_i\| = \lambda_i$ para $i = 1, 2$.*

Definição 2.25. *Sejam $v_1, v_2, \ldots, v_n$ vetores do $\mathbb{R}^n$. Consideremos*

$$V_i = \|v_i\|^2 = \langle v_i, v_i \rangle$$

A condição importante para o algoritmo de Gauss é que

$$\|v_2 - \mu v_1\|^2 = V_2 - 2\mu \langle v_1, v_2 \rangle + \mu^2 V_1$$

é mínimo quando $\mu = \frac{\langle v_1, v_2 \rangle}{V_1}$.

No caso de reticulados, podemos trocar o elemento da base v_2 por $v_2 - \lfloor \mu \rceil v_1$, onde $\lfloor \mu \rceil$ é o inteiro mais próximo de μ.

Lema. *Uma base ordenada* $\{v_1, v_2\}$ *é Gauss reduzida se, e somente se,*

$$\|v_1\| \leq \|v_2\| \leq \|v_2 \pm v_1\|$$

Algorítimo. Redução de Gauss
Entradas: base $\{v_1, v_2\}$ do reticulado Λ.
Saidas: base (v_1, v_2) de Λ tal que $\|v_i\| = \lambda_i$
$V_1 = \|v_1\|^2$
$\mu = \langle v_1, v_2 \rangle / V_1$
$v_2 = v_2 - \lfloor \mu \rceil v_1$
$V_2 = \|v_2\|^2$
Enquanto $V_2 < V_1$
Faça
Troca v_1e v_2
$V_1 = V_2$
$\mu = \langle v_1, v_2 \rangle / V_1$
$v_2 = v_2 - \lfloor \mu \rceil v_1$
$V_2 = \|v_2\|^2$
Fim da rotina Enquanto
Retorna as bases.

Exemplo. Considere a seguinte base $\{v_1, v_2\}$ onde $v_1 = (3, 8)$ e $v_2 = (5, 14)$ de um reticulado Λ.
$V_1 = \|v_1\|^2 = \left(\sqrt{9 + 64}\right)^2 = 73$
$V_2 = \|v_2\|^2 = \left(\sqrt{25 + 196}\right)^2 = 221$
$V_1 < V_2$
$\langle v_1, v_2 \rangle = 3.5 + 8.14 = 15 + 112 = 127$
$\mu = \langle v_1, v_2 \rangle / V_1 = \frac{127}{73} = 1,74$
$v_2 = v_2 - \lfloor \mu \rceil v_1 = (5, 14) - 2(3, 8) = (-1, -2)$
$V_1 = \|v_1\|^2 = 73$
$V_2 = \|v_2\|^2 = 5 \Rightarrow V_2 < V_1$
Então, $v_1 = (-1, -2)$ e $v_2 = (3, 8)$
$\mu = -3, 8$
$v_2 = v_2 - \lfloor \mu \rceil v_1 = (3, 8) + 4(-1, -2) = (-1, 0)$
$V_2 = 1 < V_1 = 5$
Então, $v_1 = (-1, 0)$ e $v_2 = (-1, -2)$
$\mu = 1$
$v_2 = (0, -2)$
$V_1 = 1 < V_2 = 2$

Logo, a base Gauss reduzida será $\begin{bmatrix} -1 & 0 \\ 0 & -2 \end{bmatrix}$

2.3.2 Redução LLL

Seja $\{v_1, \ldots, v_n\}$ uma base ordenada de um reticulado Λ, $\{v_1^*, \ldots, v_n^*\}$ a ortogonalização por Gram-Schmidt e $V_i = \|v_i^*\|^2 = \langle v_i^*, v_i^* \rangle$. Seja também $\mu_{i,j} = \langle v_i, v_j^* \rangle / \langle v_j^*, v_j^* \rangle$ o coeficiente no processo de Gram-Schmidt e $1/4 < \delta < 1$.

Uma base é LLL reduzida (com fator δ) se satisfazer as seguintes condições:

1. $|\mu_{i,j}| \leq 1/2$ com $1 \leq j \leq i \leq n$
2. $V_i \geq \left(\delta - \mu_{i,i-1}^2\right) V_{i-1}$ com $2 \leq i \leq n$ (condição de Lovász).

Como normalmente na condição de Lovász $\delta = 3/4$, podemos escrever

$\|v_i^*\|^2 \geq \left(\frac{3}{4} - \mu_{i,i-1}^2\right) \left\|v_{i-1}^*\right\|^2 \Longrightarrow \left\|v_i^* + \mu_{i,i-1} v_{i-1}^*\right\|^2 \geq \frac{3}{4} \left\|v_{i-1}^*\right\|^2$

Para aplicar a redução de base usando o método LLL, precisamos primeiro aplicar o processo de ortogonalização de Gram-Schmidt como uma subrotina do algoritmo LLL.

A seguir apresentamos o algoritmo para redução LLL baseado em Galbraith [5].

Algorítimo. Redução LLL com $\delta = 3/4$ e norma Euclidiana.

Entrada: $v_1, \ldots, v_n \in \mathbb{Z}^m$

Saida: base LLL reduzida $v_1, \ldots, v_n$.

Encontrar a base $v_1^*, \ldots, v_n^*$ pelo processo de Gram-Schmidt (chamar sub-rotina) e $\mu_{i,j}$ para $1 \leq j \leq i \leq n$.

$V_i = \langle v_i^*, v_i^* \rangle = \|v_i^*\|^2$ para $1 \leq i \leq n$

$k = 2$

Enquanto $k \leq n$ faça

para $y = (k-1)$até 1 faça

$q_j = \lfloor \mu_{k,j} \rceil$ e $v_k = v_k - q_j v_j$

atualizar $\mu_{k,j}$ para $1 \leq j < k$

fim da rotina para

Se $V_k \geq \left(\frac{3}{4} - \mu_{k,k-1}^2\right) V_{k-1}$ então $k = k + 1$

caso contrário

troca v_k com v_{k-1}

atualizar v_k^*, v_{k-1}^*, $\mu_{k-1,j}$ e $\mu_{k,j}$

para$1 \leq j < k$ e $\mu_{i,k}$, $\mu_{i,k-1}$ para $k < i \leq n$

$k = min\{2, k-1\}$

fim da rotina se

fim da rotina enquanto.

O vetor v_1 dado pela redução usando o algoritmo LLL nos oferece um vetor próximo de ser o mais curto, e em certos casos, até nos dá o mais curto, porém oficialmente não

é um algoritmo para resolver o problema do vetor mais curto (veremos mais adiante). Nota-se também que esse algoritmo nos oferece vetores com tamanhos menores ou iguais a $2^{\frac{n+1}{2}}r$.

2.3.3 Redução de Minkowski

Consideremos uma base $\beta = \{u, v\}$ de um reticulado Λ. Dizemos que β é **Minkowski reduzida** se satisfazer as condições de Minkowski, ou seja,

$$\langle u, u\rangle \leq \langle v, v\rangle \ \ e \ \ |\langle u, v\rangle| \leq \frac{\langle u, u\rangle}{2}.$$

Teorema 2.26. *Se $\{a_1, a_2\}$ é base Minkowski reduzida, então $\|a_1\|_2 = \lambda_1$.*

Uma base Minkowski reduzida contém o menor vetor de um reticulado. Um algoritmo para encontrar uma base Minkowski-reduzida é dada por Conway and Sloane [3].

Algorítimo. Redução de Minkowski para dimensão 2.

se $\|a_1\|_2 > \|a_2\|_2$ troque a_1 e a_2

$r \to 0$

Enquanto $\|r\|_2 < \|a_1\|_2$ faça

$a_2 \leftarrow a_1$

$a_1 \leftarrow r$

$w \leftarrow \left\lfloor \frac{\langle a_1, a_2\rangle}{\langle a_1, a_1\rangle} \right\rceil$

$r \leftarrow a_2 - wa_1$

fim da rotina Enquanto

retorna $\{a_1, a_2\}$.

Para dimensões maiores não se tem um algoritmo que faça a redução de Minkowski de forma eficiente.

2.4 Problema do vetor mais curto e do vetor mais próximo

Os assuntos abordados nesta seção são sobre os problemas do vetor mais curto (SVP) e do vetor mais próximo (CVP) e têm como principais referências Galbraith [5] e Fincke and Pohst [4].

2.4.1 O Problema do vetor mais curto

Dado um reticulado Λ, o **problema do vetor mais curto - SVP (shortest vector problem)**- consiste em, dado uma base B de Λ, encontrar um vetor não nulo $v \in \Lambda$ tal que $\|v\|$ é mínimo ($\|v\| = \lambda_1$).

Uma variação para esse problema é o Problema do vetor mais curto aproximado (ASVP) que consiste em dado uma base B de Λ, encontrar um vetor não nulo $v \in \Lambda$ tal que $\|v\| \leq \gamma\lambda_1$ com $\gamma > 1$.

Existem vários algoritmos que tentam resolver esse problema. Neste trabalho será apresentado o algoritmo proposto por Fincke and Pohst [4].Esse algoritmo usa o método de Cholesky para transformar uma matriz positiva definida na forma quadrática X^tAX com $X \in \mathbb{R}^{m\times 1}$, onde $A = B^tB$, de $X^tB^tBX \leq C$ (C constante positiva) em uma soma, ou seja, $X^tAX = \sum_{i,j=1}^{m} a_{ij}x_ix_j$ transforma-se em

$$Q(x) := \sum_{i=1}^{m} q_{ii}\left(x_i + \sum_{j=i+1}^{m} q_{ij}x_j\right)^2. \tag{2.4}$$

Executando os seguintes passos:

$$q_{ij} \leftarrow a_{ij}\ (1 \leq i \leq j \leq m)$$

$$\text{para } i = 1, 2, \ldots, m-1$$

$$q_{ji} \leftarrow q_{ij},\ q_{ij} \leftarrow \frac{q_{ij}}{q_{ii}}\ (i+1 \leq j \leq m)$$

$$\text{para todo } i \text{ e } k = i+1, \ldots, m$$

$$q_{kl} \leftarrow q_{kl} - q_{ki}q_{il}\ (k \leq l \leq m)$$

Para encontrar os valores do R, sabe-se que a saida será semelhante aos passos dados em 2.4 e as entradas r_{ij} de R são:

$$r_{ij} = 0\ (1 \leq j \leq i \leq m),$$

$$r_{ii} = q_{ii}^{1/2}\ (1 \leq i \leq m)\ (5)$$

$$r_{ij} = r_{ii}q_{ij}\ (1 \leq i \leq j \leq m)$$

Transforma-se X^tAX em $Q(x)$ e então resolvesse $Q(x) \leq C$. Isto é feito utilizando o seguinte algoritmo:

Algorítimo 2.27. Para resolver $Q(x) \leq C$

Entradas: $q_{ij}\ (1 \leq i \leq j \leq m)$, $Q(x)$ e $C > 0$.
Saídas: todo $x \in \mathbb{Z}^m$, $x \neq 0$ e $Q(x) \leq C$.

1. (Inicialização) $i \leftarrow m\ T_i \leftarrow C,\ U_i \leftarrow 0$.

2. (limitantes para x) $Z \leftarrow (T_i/q_{ii})^{1/2}$, $UB(x_i) \leftarrow \lfloor Z - U_i \rfloor$ e $x_i \leftarrow \lceil -Z - U_i \rceil - 1$.

3. (Incrementa x_i) $x_i \leftarrow x_i+1$, **Para** $x_i \leq UB(x_i)$ vai para o passo 5, **Caso contrário** vai para 4.

4. (Incrementa i) $i \leftarrow i+1$ e volta para 3.

5. (Diminui i) **Para** $i=1$ vai para 6, **Caso contrário** $i \leftarrow i-1$, $U_i \leftarrow \sum_{j=i+1}^{m} q_{ij}x_j$, $T_i \leftarrow T_{i+1} - q_{i+1,i+1}(x_{i+1}+U_{i+1})^2$.

6. (Solução encontrada) Para $x=0$ terminar a rotina. **Caso contrário** mostrar x, $-x$, $Q(x) = C - T_1 + q_{11}(x_i+U_i)^2$ e volta para 3.

E em seguida o algorítmo para resolver $X^tAX \leq C$, que terá como sub-rotina o algorítmo 2.25.

Algorítimo. Algoritmo para resolver $X^tAX \leq C$
Entradas: $A \in \mathbb{R}^{m\times m}$ positiva definida e $C > 0$;
Saídas: todo $x \in \mathbb{Z}^m$, $x \neq 0$ e $X^tAX \leq C$;

1. (Decomposição de Cholesky de A) Computa a matriz triangular superior R, R^{-1} de A por 2.4 e 2.4.1.

2. (Redução) Computa redução da linha S^{-1} de R^{-1} assim como U^{-1}, onde $S^{-1} = U^{-1}R^{-1}$ e faz $S = RU$.

3. (Reordena as colunas de S) determina a permutação π tal que $\left\|S'_{\pi(1)}\right\| \geq \left\|S'_{\pi(2)}\right\| \geq \ldots \geq \left\|S'_{\pi(m)}\right\|$ onde $S'_{\pi^{-1}(i)}$ $1 \leq i \leq m$ são colunas da matriz s.

4. (Decomposição de Cholesky de S^tS) Computa a matriz triângular superior $Q = (q_{ij})$ de S^tS 2.4.

5. (Aplicação de 2.27) Computa todas as soluções $y \in \mathbb{Z}^m$, $y \neq 0$, $Q(y) \leq C$ de 2.27 e retorna $X = U\left(y_{\pi^{-1}(1)}, \ldots, y_{\pi^{-1}(m)}\right)^t$para cada y.

No algoritmo apresentado no capítulo 4 foi feito uma alteração no algoritmo SVP porque neste último usa-se a decomposição de Cholesky que por sua vez trabalha com a matriz de Gram. Como foi referido no capítulo 2, a matriz de Gram independe da base usada, ou seja, se por exemplo pegarmos uma base e rotacionarmos continuamos com a mesma matriz de Gram. Na norma p a rotação muda o tamanho do vetor da base, e isso não seria levado em consideração pela decomposição de Cholesky. Por esses motivos optou-se por Trocar a decomposição de Cholesky pela forma normal de Hermite.

2.4.2 O Problema do vetor mais próximo

Dado um reticulado Λ, o **problema do vetor mais próximo - CVP (closest vector problem)**- consiste em, dado uma base B de Λ e vetor $w \in \mathbb{Q}^m$, encontrar um vetor $v \in \Lambda$ tal que $\|w - v\|$ seja mínimo.

Para esse problema também existe uma variação chamada de Problema do vetor mais próximo aproximado (ACVP) que consiste em dado uma base B de um reticulado Λ e um vetor $w \in \mathbb{Q}^m$, encontrar $v \in \Lambda$ tal que, $\|w - v\| < \gamma \|w - xB\|$ para qualquer $x \in \mathbb{Z}^n$ e $\gamma > 1$.

Capítulo 3

Códigos

Uma parte importante na teoria da informação é a teoria dos códigos, que teve como marco importante o trabalho de Shannon em 1948, "A mathematical theory of communication". Codificar é converter algum dado em outra forma de comunicação. Por exemplo, utilizamos códigos quando armazenamos algum dado num computador. Para acessar esses dados o computador faz o processo inverso da decodificação. Outro exemplo de código é a própria linguagem escrita, o alfabeto. As referências para este capítulo são Silva [11], Strapasson [12], Hefez and Vilella [7], Jorge et al. [9], Campello [1], Strapasson et al. [13]

3.1 Códigos corretores de erros

Um dos grandes desafios na codificação/decodificação de uma informação é transmitir a informação com a menor margem de erro possível. Segundo Hefez e VillelaHefez and Vilella [7], código corretor é uma forma organizada de acrescentar dados a cada informação que se pretende transmitir de modo a conseguir posteriormente não somente recuperar a informação, mas também detectar e corrigir erros.

Uma das construções mais utilizadas, no tocante a códigos corretores de erros é a construção A, que relaciona um código corretor de erro em $\mathbb{Z}_q^n$ e um reticulado em $\mathbb{Z}^n$. Os reticulados obtidos pela construção A são chamados de q-ários.

Vamos considerar corpos finitos $\mathbb{Z}_q$(onde q é primo). Designamos $\mathbb{Z}_q = \left\{\overline{0}, \overline{1}, \ldots, \overline{q-1}\right\}$. Utilizaremos o espaço vetorial $\mathbb{Z}_q^n$ que é o conjunto de todas as n-uplas de elementos $\mathbb{Z}q$.

Um código C sobre $\mathbb{Z}_q$ é um subconjunto de $\mathbb{Z}_q^n$, onde $\mathbb{Z}_q$ é chamado de *alfabeto* e os elementos de C são chamados de *palavras*. Um código C munido de uma métrica d possui três parâmentros considerados fundamentais, representados da seguinte forma: $[n, M, d]$. Neste caso o n representa o comprimento do código, M representa o seu número de elementos e d representa a sua distância mínima. Os códigos ditos bons (que mais interessam) são aqueles onde os valores de M e d são grandes em relação ao n.

Podemos definir um código C como **código linear** se for um subespaço vetorial de $\mathbb{Z}_q^n$.

Definição 3.1. *A **distância mínima** de um código C é dado pelo número*

$$d = min\left\{d\left(u,v\right) : u,v \in C \, e \, u \neq v\right\}$$

É de suma importância o cálculo da distância de um código, pois quanto maior for a distância mínima de um código, maior é a capacidade de correção de erro.

Teorema. *Seja C um código com distância mínima d. Então C pode corrigir até $k = \left[\frac{d-1}{2}\right]$ erros e detectar até $d-1$ erros.*

Definição 3.2. *O código dual, ou ortogonal, é dado por*

$$C^* = \left\{x \in \mathbb{Z}_q^n : \, \langle x, \overline{u} \rangle = 0, \, \forall u \in C\right\}$$

Um código C é dito auto-dual se $C = C^*$.

3.2 Métrica de Hamming

A métrica de Hamming foi definida em 1950 e é uma das formas de medir a distância entre as palavras que faremos refencia neste trabalho.

Definição 3.3. *Dados u e v, dois elementos de $\mathbb{Z}_q^n$, onde $u = (u_1, u_2, \ldots, u_n)$ e $v = (v_1, v_2, \ldots, v_n)$, a distância de Hamming é definida como:*

$$d_H\left(u,v\right) = \left|\{i : u_i \neq v_i, 1 \leq i \leq n\}\right|$$

A distância de Hamming também pode ser chamada de métrica de Hamming.

Consideremos um alfabeto $\mathbb{Z}_q$ e um número natural n. Dizemos que uma função $F : \mathbb{Z}_q^n \to \mathbb{Z}_q^n$ é isometria de $\mathbb{Z}_q^n$ se ela preservar a distância de Hamming, ou seja,

$$d_H\left(F\left(x\right), F\left(y\right)\right) = d_H\left(x,y\right), \forall x,y \in \mathbb{Z}_q^n.$$

Definição 3.4. *Dado $x \in \mathbb{Z}_q^n$, o **peso** de x é o número inteiro dado por*

$$\omega\left(x\right) := \left|\{i : x_i \neq 0\}\right|$$

ou seja , $\omega\left(x\right) = d_H\left(x,0\right)$.

O peso de um código linear C é dado por

$$\omega\left(C\right) := min\left\{\omega\left(x\right) : x \in C \setminus \{0\}\right\}$$

3.3 Métrica de Lee

A **distância de Lee**, d_{Lee}, entre dois pontos $x, y \in \mathbb{Z}_q^n$ é dada por

$$d_{Lee}(\overline{x}, \overline{y}) = min\{|x-y|, q-|x-y|\}$$

Neste caso, a métrica denominada de métrica de Lee é dada por

$$d_{Lee}(\overline{x}, \overline{y}) = d_{Lee}((x_1, \ldots, x_n), (y_1, \ldots, y_n)) := \sum_{i=0}^{n} min\{|x_i - y_i|, q-|x_i - y_i|\}$$

$$= \sum_{i=0}^{n} d_{Lee}(\overline{x_i}, \overline{y_i})$$

Se considerarmos um poligono regular de p lados, a distância de Lee entre dois pontos é o menor número de arestas desse polígono que se percorre para ligar dois vértices $\overline{x}$ *e* $\overline{y}$.

O peso de Lee de um elemento $x \in \mathbb{Z}_q^n$ é dado por $\omega_{Lee}(x) = d_{Lee}(x, 0)$.

Para $q = 2$ ou $q = 3$ a métrica de Lee coincide com a métrica de Hamming.

3.4 Códigos Perfeitos e quase-perfeitos na métrica de Lee

Dado um código C com raio de empacotamento r , consideramos todas as bolas centradas nos pontos do código e de raio r. Ao recebermos uma mensagem verificamos em qual das bolas a mensagem recebida se encontra e corrigimos o erro assumindo que a mensagem enviada é a mais próxima da recebida, isto é mais próxima do centro da bola em questão. Em algumas situações a mensagem recebida não pertence a nenhuma das bolas referidas acima. Neste caso, temos um problema! Porém, se o nosso código for perfeito, essa situação não poderá ocorrer, ou seja a mensagem recebida estará sempre dentro de alguma bola de centro nos pontos do código e raio r.

Vamos considerar um elemento $a \in \mathbb{Z}_q^n$, um número real r positivo e uma métrica d . Podemos então definir uma bola e uma esfera de centro em a e raio r respectivamente como:

$$B(a, r) = \left\{u \in \mathbb{Z}_q^n : \ d(u, a) \leq r\right\}$$

$$S(a, r) = \left\{u \in \mathbb{Z}_q^n : \ d(u, a) = r\right\}$$

Definição 3.5. *Um código C é dito* ***perfeito*** *se*

$$\bigcup_{u \in C} B(u, r) = \mathbb{Z}_q^n$$

e

$$B(u,r) \bigcap B(v,r) = \emptyset \; e \; u \neq v$$

Em outras palavras, um código pertencente a $\mathbb{Z}^n$ é dito perfeito com raio r, se para cada ponto x também pertencente a $\mathbb{Z}^n$, existe um único y pertencente a esse código tal que a distância entre x e y $(d(x,y))$ seja menor ou igual ao raio r.

Num código perfeito o raio de empacotamento é igual ao raio de cobertura.

Um código é chamado de **quase-perfeito** se a união de todas as bolas centradas nas palavras do código não cobrir todos os pontos inteiros do $\mathbb{Z}^n$, ou seja, existe um x pertencente a $\mathbb{Z}^n$ que não pertence a nenhuma das bolas com centro nas palavras do código e com raio de empacotamento r e o raio de cobertura é o raio de empacotamento mais uma (consecutivos).

3.5 Métrica p-Lee

A métrica p-Lee é uma extensão da métrica de Lee.

A distância entre dois pontos de $\mathbb{Z}^n$ considerando a norma l_p ao invés da norma euclidiana, é dada por:

$$d_p(x,y) := \left(\sum_{i=1}^{n} |x_i - y_i|^p \right)^{\frac{1}{p}}$$

para $1 \leq p < \infty$.

Se considerarmos dois vetores $\overline{x}$ e $\overline{y}$ pertencentes a $\mathbb{Z}_q^n$, podemos então definir a distância p-Lee como sendo

$$d_{p,Lee}(\overline{x},\overline{y}) = \left(\sum_{i=1}^{n} \left(d_{Lee}(\overline{x_i},\overline{y_i})\right)^p \right)^{\frac{1}{p}}$$

para $1 \leq p < \infty$.

Nota-se que a métrica de Lee é a métrica p-Lee para $p = 1$.

Como em qualquer métrica, a distância mínima é a menor distância de um código C. Usando a métrica p-Lee, podemos defini-la da seguinte forma:

$$d_{p,Lee}(C) = \min_{\overline{x},\overline{y} \in C, \overline{x} \neq \overline{y}} d_{p,Lee}(\overline{x},\overline{y})$$

Definição 3.6. *Definimos o conjunto das distâncias em $\mathbb{Z}^n$, na métrica l_p, como sendo*

$$D_{p,n} = \{d \in \mathbb{R} \; tal \; que, \; existe \; z \in \mathbb{Z}^n \; e \; c \in C \; com \; d_p(z,c) = d\}.$$

Uma bola é definida na métrica p-Lee como sendo

$$B_{p,Lee}(\overline{x}, r) = \left\{\overline{y} \in \mathbb{Z}_q^n : \ d_{p,Lee}(\overline{x}, \overline{y}) \leq r\right\}$$

onde r é o raio de empacotamento de um código C e é dado pelo maior raio $r \in D_{p,n}$ tal que as seguintes condições sejam cumpridas:

1. $B_{p,Lee}(\overline{x}, r) \bigcap B_{p,Lee}(\overline{y}, r) = \emptyset \ \forall \overline{x}, \overline{y} \in C$ e $\overline{x} \neq \overline{y}$.
2. Existe $\overline{x} \in C$ e $\overline{y} \in \mathbb{Z}_q^n$ tais que $d_{p,Lee}(\overline{y}, \overline{x}) = r$.

Na métrica l_p o raio de empacotamento será designado por r_p. O r^p é sempre um inteiro que podemos escrever como a soma de inteiros elevados a p.

Exemplo 3.7. Para $p = 2$, um possível raio seria $r = \sqrt{5}$, pois $5 = 2^2 + 1^2$. Para $p = 3$ um possível raio seria $r = \sqrt[3]{9}$, pois $9 = 2^3 + 1^3$.

O raio de cobertura de um código na métrica l_p, R_p, por sua vez, é dado pelo menor raio $r \in D_{p,n}$ tal que

$$\bigcup_{\overline{x} \in C} \overline{x} + B_p^n(r) = \mathbb{Z}^n$$

Os raios de empacotamento e de cobertura contínuo de um reticulado Λ serão designados por $\overline{r_p}$ e $\overline{R_p}$ respectivamente. Para o raio de empacotamento $\overline{r_p}$ as bolas centradas nos pontos do reticulado Λ e com raio $\overline{r_p}$ não se interceptam em $\mathbb{R}^n$ e para o raio de cobertura $\overline{R_p}$ a união das bolas com centro nos pontos do reticulado Λ e com raio $\overline{R_p}$ cobrem o $\mathbb{R}^n$ totalmente.

Se olharmos o caso contínuo, as bolas centradas nos pontos do reticulado com raio $\overline{r_p}$ não se interceptam, porém na cobertura, a união das bolas centradas nos pontos do reticulados e com raio $\overline{R_p}$ cobrem totalmente o espaço do $\mathbb{R}^n$.

Exemplo 3.8. Na figura 3.1, os raios de empacotamento para os casos discreto e contínuo são dados respectivamente por $r_p = \sqrt{2}$ e $\overline{r_p} = 2$.

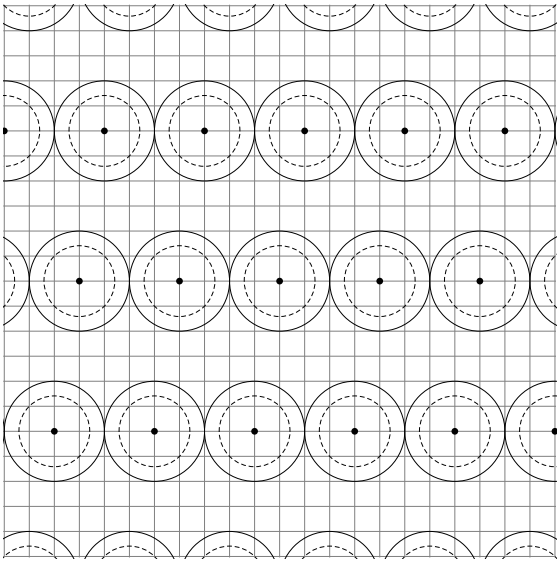

Figura 3.1: Exemplo de bolas de empacotamento contínuo e discreto

Exemplo 3.9. Na figura 3.2, os raios de cobertura para os casos discreto e contínuo são dados respectivamente por $R_p = 3,1623$ e $\overline{R_p} = 3,4004$.

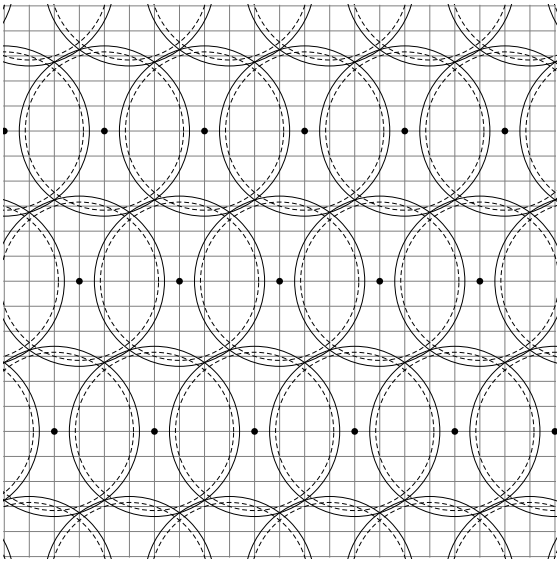

Figura 3.2: Exemplo de bolas de cobertura contínuo e discreto

Se considerarmos a união de cubos unitários em $\mathbb{R}^n$ centrados nos pontos de $B_p^n(r)$ (bola na métrica l_p), $1 \leq p < \infty$, produzimos uma figura chamada de **Poliominó**. Considerando também um ladrilhamento de $\mathbb{Z}^n$ pela translação da bola $B_p^n(r)$, induzimos um ladrilhamento do $\mathbb{R}^n$ pelos poliominós correspondentes, expresso da seguinte forma:

$$T_p^n := \bigcup_{x \in B_p^n(r)} \left(x + \left[-\frac{1}{2}, \frac{1}{2} \right]^n \right), \; 1 \leq p < \infty$$

Exemplo 3.10. Exemplo de poliominó

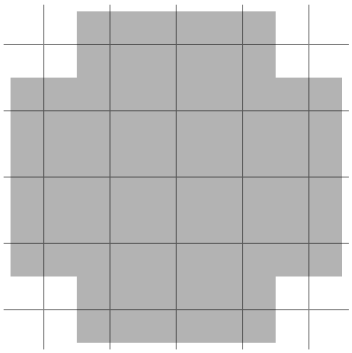

Figura 3.3: Poliominó

Capítulo 4

Grau de imperfeição

Este capitulo é dedicado à explanação do trabalho de Strapasson et al. [13].

4.1 Grau de Imperfeição

Antes de definirmos o grau de imperfeição, precisamos fazer a definição seguinte.

Definição 4.1. *A distância entre dois elementos $x, y \in D_{p,n}$ e $x < y$, é definida como sendo $d(x,y) = \#(D_{p,n} \bigcap [x,y))$ onde $[x,y)$ é o intervalo em $\mathbb{R}$ e $d(x,x) = 0$.*

Podemos então definir o grau de imperfeição, denotado por t da seguinte forma:

Definição 4.2. *Strapasson et al. [13] Dizemos que um reticulado Λ tem **grau de imperfeição** t se a distância entre o raio de empacotamento e de cobertura for igual a t, ou seja, $d(r_p, R_p) = t$.*

Quando o raio de empacotamento e de cobertura forem iguais, então a distância entre eles é zero. Isto acontece quando o reticulado for perfeito. No caso do reticulado quase-perfeito, como os raios de empacotamento e cobertura são consecutivos, a distância entre eles é 1.

Sabendo que a densidade de empacotamento é limitada por um valor máximo designado por $\overline{\Delta_p^n}$, o raio de empacotamento de um código linear na métrica l_p, também é limitado por Strapasson et al. [13]

$$r_p \leq \frac{\sqrt[p]{n}}{2} \frac{\left(1 + \sqrt[n]{\overline{\Delta_p^n}}\right)}{\left(1 - \sqrt[n]{\overline{\Delta_p^n}}\right)}$$

Onde $\overline{\Delta_p^n}$ é a densidade de empacotamento contínuo de um reticulado na metrica l_p e na dimensão n.

A densidade de cobertura contínua de um reticulado é definidada na métrica l_p como sendo

$$\overline{\Theta_p^n}(\Lambda) = \frac{V_p^n \overline{R_p^n}}{det\Lambda}$$

onde V_p^n é o volume da esfera unitária de dimensão n centrada na origem.

Proposição 4.3. *Strapasson et al. [13] Sejam $1 < p < \infty$ e $n \geq 2$. O raio de cobertura R_p e o raio de empacotamento r_p de um código linear quase- perfeito na métrica l_p, satisfazem*

$$\overline{\Theta_p^n} \leq \frac{V_p^n \left(R_p + \frac{1}{2}\sqrt[p]{n}\right)^n}{\left|B_p^n(r_p)\right|}$$

e

$$\overline{\Theta_p^n} \leq \frac{V_p^n \left(r_p + \sqrt[p]{n}\right)^n}{\left|B_p^n(r_p)\right|}$$

Definimos $\mu(n,p,r)$ como sendo a cardinalidade do conjunto $B_p^n(r) \bigcap \mathbb{Z}^n$, ou seja, é o volume da bola de raio r centrada na origem.

A densidade de empacotamento discreto de um reticulado Λ em $\mathbb{Z}^n$e na métrica l_p é dada por

$$\Delta_p^n(\Lambda) = \frac{\mu(n,p,r_p)}{(\det\Lambda)^{1/2}},$$

E a densidade de cobertura discreta é dada por

$$\Theta_p^n(\Lambda) = \frac{\mu(n,p,R_p).}{(\det\Lambda)^{1/2}}$$

Exemplo 4.4. Na tabela da figura 4.1 é apresentado um exemplo com todos os reticulados inteiros em $\mathbb{Z}^2$, tirando os casos de congruências, cujos determinantes valem 30. Também é mostrado os raios de empacotamento contínuo $\overline{r_p}$ e discreto r_p , os raios de cobertura discreto R_p e contínuo $\overline{R_p}$, as densidade de empacotamento contínuo $\overline{\Delta_p^n}$ e discreto Δ_p^n, as densidades de cobertura contínuo $\overline{\Theta_p^n}$ e discreto Θ_p^n e o grau de imperfeição t de cada um deles. Nota-se que neste caso não existem códigos perfeitos ou quase-perfeitos.O melhor que se conseguiu foram reticulados com grau de imperfeição $t = 2$.

Reticulado	Grau de imperfeição	r_p	$\overline{r}_p$	R_p	$\overline{R}_p$	Δ_p	$\overline{\Delta}_p$	Θ_p	$\overline{\Theta}_p$
$\begin{pmatrix} 1 & 0 \\ 0 & 30 \end{pmatrix}$	86.	0.	0.5	15.	15.0083	0.0333	0.0262	23.6333	23.5881
$\begin{pmatrix} 1 & 1 \\ 0 & 30 \end{pmatrix}$	48.	0.	0.7071	10.6301	10.6301	0.0333	0.0524	11.9	11.8333
$\begin{pmatrix} 1 & 2 \\ 0 & 30 \end{pmatrix}$	21.	1.	1.118	6.7082	6.8007	0.1667	0.1309	4.8333	4.8433
$\begin{pmatrix} 1 & 3 \\ 0 & 30 \end{pmatrix}$	11.	1.4142	1.5811	5.	5.	0.3	0.2618	2.7	2.618
$\begin{pmatrix} 1 & 4 \\ 0 & 30 \end{pmatrix}$	7.	2.	2.0616	4.1231	4.1254	0.4333	0.4451	1.9	1.7822
$\begin{pmatrix} 1 & 5 \\ 0 & 30 \end{pmatrix}$	3.	2.8284	2.5495	3.6056	3.6056	0.8333	0.6807	1.5	1.3614
$\begin{pmatrix} 1 & 6 \\ 0 & 30 \end{pmatrix}$	3.	2.8284	2.5	3.6056	3.6553	0.8333	0.6545	1.5	1.3992
$\begin{pmatrix} 1 & 7 \\ 0 & 30 \end{pmatrix}$	5.	2.	2.2361	3.6056	3.7268	0.4333	0.5236	1.5	1.4544
$\begin{pmatrix} 1 & 8 \\ 0 & 30 \end{pmatrix}$	5.	2.	2.2361	3.6056	4.0311	0.4333	0.5236	1.5	1.7017
$\begin{pmatrix} 1 & 9 \\ 0 & 30 \end{pmatrix}$	5.	2.	2.1213	3.6056	3.8833	0.4333	0.4712	1.5	1.5792
$\begin{pmatrix} 1 & 10 \\ 0 & 30 \end{pmatrix}$	12.	1.4142	1.5	5.099	5.1245	0.3	0.2356	2.9667	2.7499
$\begin{pmatrix} 1 & 11 \\ 0 & 30 \end{pmatrix}$	7.	2.	2.1213	4.1231	4.1231	0.4333	0.4712	1.9	1.7802
$\begin{pmatrix} 1 & 12 \\ 0 & 30 \end{pmatrix}$	2.	2.8284	2.5	3.1623	3.5355	0.8333	0.6545	1.2333	1.309
$\begin{pmatrix} 1 & 13 \\ 0 & 30 \end{pmatrix}$	5.	2.	2.2361	3.6056	3.7268	0.4333	0.5236	1.5	1.4544
$\begin{pmatrix} 1 & 14 \\ 0 & 30 \end{pmatrix}$	12.	1.	1.4142	5.	5.4203	0.1667	0.2094	2.7	3.0767
$\begin{pmatrix} 1 & 15 \\ 0 & 30 \end{pmatrix}$	24.	0.	1.	7.0711	7.5333	0.0333	0.1047	5.3667	5.943
$\begin{pmatrix} 2 & 0 \\ 0 & 15 \end{pmatrix}$	24.	0.	1.	7.0711	7.5664	0.0333	0.1047	5.3667	5.9952
$\begin{pmatrix} 2 & 3 \\ 0 & 15 \end{pmatrix}$	8.	2.	1.8028	4.2426	4.3566	0.4333	0.3403	2.0333	1.9876
$\begin{pmatrix} 2 & 5 \\ 0 & 15 \end{pmatrix}$	2.	2.8284	2.6926	3.1623	3.4482	0.8333	0.7592	1.2333	1.2451
$\begin{pmatrix} 2 & 6 \\ 0 & 15 \end{pmatrix}$	3.	2.2361	2.5	3.1623	3.5355	0.7	0.6545	1.2333	1.309
$\begin{pmatrix} 3 & 0 \\ 0 & 10 \end{pmatrix}$	12.	1.4142	1.5	5.099	5.2202	0.3	0.2356	2.9667	2.8536
$\begin{pmatrix} 3 & 5 \\ 0 & 10 \end{pmatrix}$	2.	2.8284	2.9155	3.1623	3.4	0.8333	0.8901	1.2333	1.2106
$\begin{pmatrix} 5 & 0 \\ 0 & 6 \end{pmatrix}$	3.	2.8284	2.5	3.6056	3.9051	0.8333	0.6545	1.5	1.597

Figura 4.1: Códigos em $\mathbb{Z}^2$ e $p = 2$ e seus respectivos graus de imperfeição, t

4.1.1 Grau de Imperfeição e densidade de empacotamento discreto

Nesta seção será mostrado algumas famílias de reticulados com um certo grau de imperfeição na métrica l_p de acordo com Strapasson et al. [13].

1. O primeiro caso é para r e p inteiros, onde $r > 1$ e $p \geq \frac{ln2}{ln\left(\frac{r}{r-1}\right)}$.

   Neste caso, o reticulado com base $\{(r, 2r-1), (2r, -1)\}$ é quase-perfeito para $r = 2$

e $r = 3$, ou seja o grau de imperfeição é 1. Para valores de $r \geq 3$ o grau de imperfeição é dado por $(r-2)$. A sua densidade de empacotamento discreto é dado por

$$\Delta_p^2(\Lambda) = \frac{(2r-1)^2 + 4}{4r^2 - r}$$

2. Caso r inteiro, $p < \frac{ln2}{ln\left(\frac{r}{r-1}\right)}$ e $(r-1)^p + (r-2)^p \leq r^p$

   O reticulado com base $\{(r-1, 2r-1), (2r, -1)\}$ tem grau de imperfeição $(r-1)$e densidade de empacotamento discreto igual a

$$\Delta_p^2(\Lambda) = \frac{(2r-1)^2}{4r^2 - r - 1}$$

3. Caso r não for inteiro e $p < \frac{ln2}{ln\left(\frac{r}{\lfloor r \rfloor}\right)}$, $\lfloor r \rfloor^p + \lfloor r-1 \rfloor^p \leq r^p$ e $2\lfloor r \rfloor^p \leq \lfloor r+1 \rfloor^p$

   O reticulado com base $\{(2\lfloor r \rfloor + 1, -1), (2\lfloor r \rfloor - 1, 2\lfloor r \rfloor)\}$ tem grau de imperfeição 1, ou seja é quase-perfeito e a densidade de empacotamento discreto é dado por

$$\Delta_p^2(\Lambda) = \frac{(2\lfloor r \rfloor + 1)^2 - 4}{4\lfloor r \rfloor^2 + 4\lfloor r \rfloor - 1}$$

4. Caso r não inteiro, $\lfloor r \rfloor^p + \lfloor r-1 \rfloor^p > r^p$, $\lfloor r \rfloor^p + \lfloor r-2 \rfloor^p \leq r^p$ e $2\lfloor r \rfloor^p \leq \lfloor r+1 \rfloor^p$

O reticulado de base $\{(2\lfloor r \rfloor + 1, -2), (2\lfloor r \rfloor - 2, 2\lfloor r \rfloor - 1)\}$ tem grau de imperfeição 2 e densidade de empacotamento discreto igual a

$$\Delta_p^2(\Lambda) = \frac{(2\lfloor r \rfloor + 1)^2 - 12}{4\lfloor r \rfloor^2 + 4\lfloor r \rfloor - 5}$$

4.2 Lista de reticulados quase-perfeitos

Nesta seção é apresentado o algoritmo de Strapasson et al. [13] para encontrar códigos perfeitos e quase-perfeitos. Mostra-se também os testes efetuados neste algoritmo para verificar o empacotamento e a cobertura. Caso se verificam os dois casos, o algoritmo devolve o reticulado "encontrado". Ainda nesta seção são apresentadas listas de reticulados quase perfeitos para n=2 e 3 nas métricas l_2 e l_3.

4.2.1 O Algoritmo

Em Strapasson et al. [13] é apresentado um algoritmo que busca todos os códigos perfeitos e quase-perfeitos em $\mathbb{Z}^n$ na métrica l_p, com $2 \leq p < \infty$. Antes de realizar a busca propriamente dita precisa-se listar os raios possíveis para os valores de p e n desejados.

Lembramos que os valores do r^p são sempre a soma de inteiros na potência p. Posteriormente, dado um certo volume M, deve se listar todos os reticulados que são possíveis com esse volume M, sendo que esse valor corresponde exatamente ao determinante do reticulado. Para facilitar esse processo recorre-se à forma normal de Hermite. Mas um cuidado pode ser tomado ao evitarmos redundâncias. Para esse caso, recorre-se as formas Hermite e simetrias.

Algorítimo 4.5. Encontrando códigos perfeitos e quase-perfeitos

entradas: M=volume do reticulado; n=dimensão; $p \in \mathbb{N}$, métrica l_p.

saidas: lista dos reticulados perfeitos e quase-perfeitos com volume M.

inicializações;

$r_p \leftarrow max\, r \in Dp, n\ \left\{r; \#B_p^n(r) \leq M\right\}$;

$R_p \leftarrow max\, r \in Dp, n\ \left\{r; \#B_p^n(r) > M\right\}$;

Lattices$\leftarrow\{\Lambda$; Λsubreticulados de $\mathbb{Z}^n$ com volume M$\}$;

DenseLattices$\leftarrow\{\}$;

Quasiperfect$\leftarrow\{\}$;

C$\leftarrow\{\}$;

Enquanto $C \leq$ #Lattices **Faz**

Se"Teste de injetividade no c-ésimo elemento de Lattices for positivo"

Então

coloca o c-ésimo elemento de Lattices em DenseLattices

C$\leftarrow$C+1;

C$\leftarrow$1;

Enquanto C$\leq$#DenseLattices **Faz**

Se" teste de cobertura" no c-ésimo elemento de DenseLattices for positivo

Então

adiciona o c-ésimo elemento de DenseLattices em Quasiperfect

C$\leftarrow$C+1;

4.2.2 Teste de injetividade e de cobertura

O algoritmo escrito acima é baseado em dois testes importantes: o chamado de "teste de injetividade" e o chamado de "teste de cobertura".

O teste de injetividade é por sua vez baseado no Teorema proposto por Horak and Albdaiwi [8] que será citado a seguir.

Teorema 4.6. *Seja $P \subset \mathbb{Z}^n$, tal que $|P| = m$. Existe um reticulado que ladrilha o $\mathbb{Z}^n$ pelo translado de P, se e somente se, existir um grupo Abeliano G de ordem m e um homeomorfismo $\phi : \mathbb{Z}^n \to G$ tal que a restrição de ϕ em P é uma bijeção.*

Em outra palavras, precisamos verificar se as bolas de raio r_p e centro nos pontos do reticulado Λ são dijuntas. Precisamos verificar se temos um empacotamento ou seja, se as bolas não se sobrepõem.

Vamos considerar um homeomorfismo $\phi : \mathbb{Z}^n \to G$, onde G é um grupo Abeliano de cardinalidade $M = det\Lambda$. Dada uma bola $B_p^n(r_p)$ e dois pontos $x, y \in B_p^n(r_p)$. Consideremos que a matriz geradora de Λ seja dada por B e que a adjunta de B seja dada por $adj(B)$. Assumimos que o isomorfismo ϕ seja uma composição de duas aplicações ϕ_1 e ϕ_2, onde $\phi_1 = xadj(B)$ e $\phi_2 = \overline{x}\,(mod\, M)$. Se aplicarmos a função ϕ sobre x e y e encontrarmos a mesma imagem, então a diferença entre os dois pertence ao núcleo de $\phi($ $ker(\phi))$ e consequentemente ao reticulado, isto é,

$$\phi(x) = \phi(y) \Leftrightarrow \phi(x - y) = 0$$

$$\therefore x - y \in ker(\phi)$$

Neste caso, $x - y = uB$, com $u \in \mathbb{Z}^n$. Se multiplicarmos ambos os lados por $adj(B)$ e sabendo que $adj(B) = B^{-1}detB$, onde B^{-1} é a inversa de B e $detB$ é o determinante da matriz B temos:

$$(x - y)\, adj(B) = uB.adj(B) = uBB^{-1}detB = udetB = uM \equiv 0 \ (mod\, M)$$

onde $M = det\Lambda = detB$.

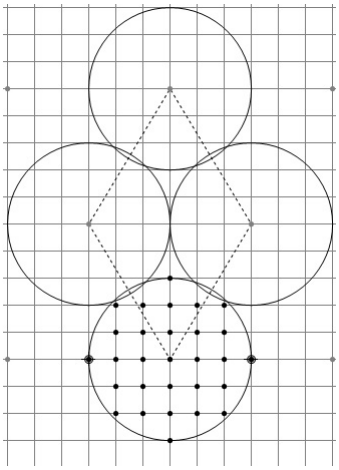

Figura 4.2: Teste de injetividade

Exemplo 4.7. Se tomarmos como exemplo o reticulado $A = \begin{pmatrix} 5 & -5 \\ 3 & 3 \end{pmatrix}$, com $M = \det A = 30$, o raio que melhor satisfaz essa relação será o $r = \sqrt{9} = 3$ que tem cardinalidade igual 29. Se olharmos para os pontos de uma bola centrada na origem e com o raio referido anteriormente teriamos o seguinte (os pares ordenados estão dispostos em linha):

$$\begin{pmatrix} -3 & 0 \\ -2 & -2 \\ -2 & -1 \\ -2 & 0 \\ -2 & 1 \\ -2 & 2 \\ -1 & -2 \\ -1 & -1 \\ -1 & 0 \\ -1 & 1 \\ -1 & 2 \\ 0 & -3 \\ 0 & -2 \\ 0 & -1 \\ 0 & 0 \\ 0 & 1 \\ 0 & 2 \\ 0 & 3 \\ 1 & -2 \\ 1 & -1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 2 \\ 2 & -2 \\ 2 & -1 \\ 2 & 0 \\ 2 & 1 \\ 2 & 2 \\ 3 & 0 \end{pmatrix}$$

exatamente os 29 números referidos anteriormente. Se pegarmos o conjunto das imagens teriamos a seguinte matriz:

$$\begin{pmatrix}
15 & 15 \\
14 & 4 \\
17 & 7 \\
20 & 10 \\
23 & 13 \\
26 & 16 \\
19 & 29 \\
22 & 2 \\
25 & 5 \\
28 & 8 \\
1 & 11 \\
21 & 21 \\
21 & 24 \\
21 & 27 \\
0 & 0 \\
3 & 3 \\
6 & 6 \\
9 & 9 \\
29 & 19 \\
2 & 22 \\
5 & 25 \\
8 & 28 \\
11 & 1 \\
4 & 14 \\
7 & 17 \\
10 & 20 \\
13 & 23 \\
16 & 26 \\
15 & 15
\end{pmatrix}$$

Se fizermos a união desse conjunto obteremos apenas 28 elementos. Isso deve-se ao fato da imagem $(15, 15)$ aparecer duas vezes, o que quer dizer que dois objetos têm a mesma imagem, a saber $(-3, 0)$ e $(3, 0)$. Isso é possível de ser visto na Figura 4.2.

A figura 4.3 ilustra o teste de cobertura.

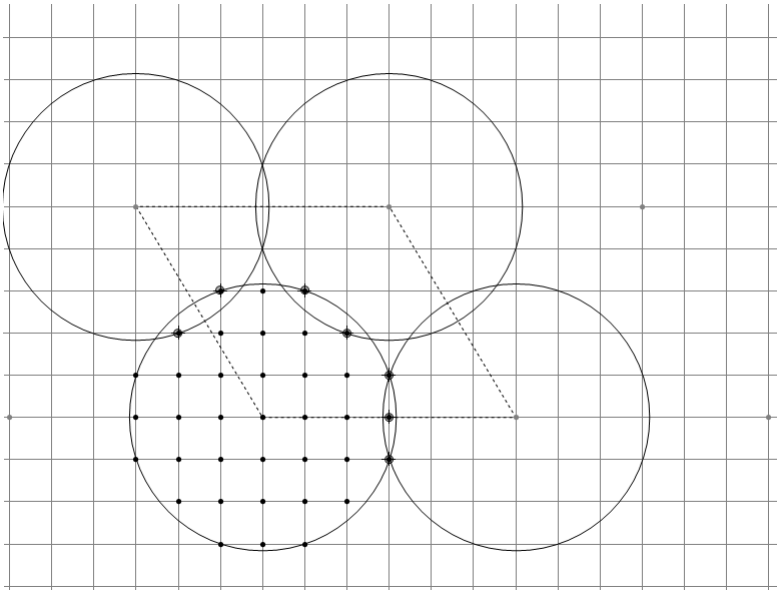

Figura 4.3: Teste de Cobertura

O teste de cobertura consiste em verificar se a região de Voronoi é um subconjunto da bola de cobertura da bola $B_p^n(R_p)$, ou seja, verificamos se as cardinalidades da região de voronoi e da bola são iguais após extrairmos as redundâncias.

Exemplo 4.8. Usando o mesmo exemplo anterior, agora para cobertura, precisamos encontrar na lista dos raios possíveis, o menor raio capaz de cobrir todos os 30 pontos. Como a cardinalidade de uma bola de raio $\sqrt{10}$ é 37, então esse seria o menor raio, já que $\sqrt{9}$ tem cardinalidade menor que 30. Neste caso precisamos verificar todos os pontos que estão na interseção dessa bola com três das bolas que a interceptam (só precisamos verificar estas porque nas outras as imagens são reflexões dessas). Se for contado o número de ponto na interseção totalizamos 7. Se forem retirados esses pontos, a cardinalidade da bola de cobertura será exatamente 30 que é o nosso M.

4.2.3 Lista de reticulados perfeitos e quase-perfeitos

Nas tabelas 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13, 4.14, 4.15, 4.16 e 4.17 são apresentadas listas de matrizes geradoras de códigos perfeitos e quase-perfeitos nas dimensões 2 e 3, para $p = 2$ e $p = 3$. Apresentamos também os respectivos raios de empacotamento r_p e cobertura R_p, assim como as cardinalidades das bolas de empacotamento $\#B_p^n(r_p)$ e de cobertura $\#B_p^n(R_p)$.

$\mathbf{p}$	**Matriz Geradora**	$\mathbf{r_p}$	$\mathbf{R_p}$	$\#\mathbf{B_p^n}(\mathbf{r_p})$	$\#\mathbf{B_p^n}(\mathbf{R_p})$	**Classificação**
2	$\begin{bmatrix} 1 & 0 \\ 2 & 5 \end{bmatrix}$	1	1	5	5	Perfeito
2	$\begin{bmatrix} 1 & 0 \\ 2 & 6 \end{bmatrix}$	1	2	5	9	Quase-Perfeito
2	$\begin{bmatrix} 1 & 0 \\ 2 & 7 \end{bmatrix}$	1	2	5	9	Quase-Perfeito
2	$\begin{bmatrix} 1 & 0 \\ 3 & 7 \end{bmatrix}$	1	2	5	9	Quase-Perfeito
2	$\begin{bmatrix} 1 & 0 \\ 3 & 8 \end{bmatrix}$	1	2	5	9	Quase-Perfeito
2	$\begin{bmatrix} 1 & 0 \\ 3 & 9 \end{bmatrix}$	2	2	9	9	Perfeito
2	$\begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}$	2	2	9	9	Perfeito
2	$\begin{bmatrix} 1 & 0 \\ 3 & 11 \end{bmatrix}$	2	4	9	13	Quase-Perfeito
2	$\begin{bmatrix} 1 & 0 \\ 4 & 11 \end{bmatrix}$	2	4	9	13	Quase-Perfeito
2	$\begin{bmatrix} 2 & 0 \\ 3 & 6 \end{bmatrix}$	2	4	9	13	Quase-Perfeito
2	$\begin{bmatrix} 1 & 0 \\ 5 & 13 \end{bmatrix}$	4	5	13	21	Perfeito
2	$\begin{bmatrix} 1 & 0 \\ 4 & 14 \end{bmatrix}$	4	5	13	21	Quase-Perfeito
2	$\begin{bmatrix} 1 & 0 \\ 4 & 15 \end{bmatrix}$	4	5	13	21	Quase-Perfeito
2	$\begin{bmatrix} 1 & 0 \\ 6 & 15 \end{bmatrix}$	4	5	13	21	Quase-Perfeito
2	$\begin{bmatrix} 1 & 0 \\ 6 & 16 \end{bmatrix}$	4	5	13	21	Quase-Perfeito
2	$\begin{bmatrix} 1 & 0 \\ 4 & 17 \end{bmatrix}$	4	5	13	21	Quase-Perfeito
2	$\begin{bmatrix} 1 & 0 \\ 5 & 17 \end{bmatrix}$	4	5	13	21	Quase-Perfeito
2	$\begin{bmatrix} 1 & 0 \\ 7 & 17 \end{bmatrix}$	4	5	13	21	Quase-Perfeito
2	$\begin{bmatrix} 1 & 0 \\ 4 & 18 \end{bmatrix}$	4	5	13	21	Quase-Perfeito
2	$\begin{bmatrix} 1 & 0 \\ 5 & 18 \end{bmatrix}$	4	5	13	21	Quase-Perfeito
2	$\begin{bmatrix} 1 & 0 \\ 7 & 18 \end{bmatrix}$	4	5	13	21	Quase-Perfeito
2	$\begin{bmatrix} 1 & 0 \\ 4 & 19 \end{bmatrix}$	4	5	13	21	Quase-Perfeito
2	$\begin{bmatrix} 1 & 0 \\ 5 & 19 \end{bmatrix}$	4	5	13	21	Quase-Perfeito

Tabela 4.1: Perfeitos e quase-perfeitos para $p = 2$ e $n = 2$

Matriz Geradora	$\mathbf{r_p}$	$\mathbf{R_p}$	$\#\mathbf{B_p^n}(\mathbf{r_p})$	$\#\mathbf{B_p^n}(\mathbf{R_p})$	**Classificação**
$\begin{bmatrix} 1 & 0 \\ 2 & 5 \end{bmatrix}$	1	1	5	5	Perfeito
$\begin{bmatrix} 1 & 0 \\ 2 & 6 \end{bmatrix}$	1	2	5	9	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 2 & 7 \end{bmatrix}$	1	2	5	9	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 3 & 7 \end{bmatrix}$	1	2	5	9	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 3 & 8 \end{bmatrix}$	1	2	5	9	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 3 & 9 \end{bmatrix}$	2	2	9	9	Perfeito
$\begin{bmatrix} 3 & 0 \\ 0 & 3 \end{bmatrix}$	2	2	9	9	Perfeito
$\begin{bmatrix} 1 & 0 \\ 3 & 11 \end{bmatrix}$	2	8	9	13	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 4 & 11 \end{bmatrix}$	2	8	9	13	Quase-Perfeito
$\begin{bmatrix} 2 & 0 \\ 3 & 6 \end{bmatrix}$	2	8	9	13	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 5 & 13 \end{bmatrix}$	8	9	13	21	Perfeito
$\begin{bmatrix} 1 & 0 \\ 4 & 14 \end{bmatrix}$	8	9	13	21	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 4 & 15 \end{bmatrix}$	8	9	13	21	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 6 & 15 \end{bmatrix}$	8	9	13	21	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 6 & 16 \end{bmatrix}$	8	9	13	21	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 4 & 17 \end{bmatrix}$	8	9	13	21	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 5 & 17 \end{bmatrix}$	8	9	13	21	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 7 & 17 \end{bmatrix}$	8	9	13	21	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 4 & 18 \end{bmatrix}$	8	9	13	21	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 5 & 18 \end{bmatrix}$	8	9	13	21	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 7 & 18 \end{bmatrix}$	8	9	13	21	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 4 & 19 \end{bmatrix}$	8	9	13	21	Quase-Perfeito

Tabela 4.2: Perfeitos e quase -perfeitos para $p = 3$ e $n = 2$

Matriz Geradora	r_p	R_p	$\#B_p^n(r_p)$	$\#B_p^n(R_p)$	Classificação
$\begin{bmatrix} 1 & 0 \\ 5 & 19 \end{bmatrix}$	8	9	13	21	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 8 & 20 \end{bmatrix}$	8	9	13	21	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 5 & 23 \end{bmatrix}$	9	16	21	25	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 9 & 23 \end{bmatrix}$	9	16	21	25	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 5 & 24 \end{bmatrix}$	9	16	21	25	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 5 & 25 \end{bmatrix}$	16	16	25	25	Perfeito
$\begin{bmatrix} 1 & 0 \\ 10 & 25 \end{bmatrix}$	16	16	25	25	Perfeito
$\begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix}$	16	16	25	25	Perfeito
$\begin{bmatrix} 1 & 0 \\ 6 & 33 \end{bmatrix}$	27	28	29	37	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 6 & 34 \end{bmatrix}$	27	28	29	37	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 10 & 35 \end{bmatrix}$	27	28	29	37	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 7 & 39 \end{bmatrix}$	28	35	37	45	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 11 & 39 \end{bmatrix}$	28	35	37	45	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 12 & 42 \end{bmatrix}$	28	35	37	45	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 7 & 47 \end{bmatrix}$	35	54	45	49	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 20 & 47 \end{bmatrix}$	35	54	45	49	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 7 & 48 \end{bmatrix}$	35	54	45	49	Quase-Perfeito
$\begin{bmatrix} 1 & 0 \\ 7 & 49 \end{bmatrix}$	54	54	49	49	Perfeito
$\begin{bmatrix} 1 & 0 \\ 14 & 49 \end{bmatrix}$	54	54	49	49	Perfeito
$\begin{bmatrix} 1 & 0 \\ 21 & 49 \end{bmatrix}$	54	54	49	49	Perfeito
$\begin{bmatrix} 7 & 0 \\ 0 & 7 \end{bmatrix}$	54	54	49	49	Perfeito

Tabela 4.3: Perfeitos e quase-perfeitos para $p = 3$ e $n = 2$ (continuação)

Matriz Geradora	$\mathbf{r_p}$	$\mathbf{R_p}$	$\#\mathbf{B_p^n(r_p)}$	$\#\mathbf{B_p^n(R_p)}$	**Classificação**
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 7 \end{bmatrix}$	1	1	7	7	Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 8 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 9 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 4 \\ 0 & 0 & 9 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 9 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 10 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 4 \\ 0 & 0 & 10 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 10 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 11 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 4 \\ 0 & 0 & 11 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 11 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 5 \\ 0 & 0 & 11 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 5 \\ 0 & 0 & 11 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & 5 \\ 0 & 0 & 11 \end{bmatrix}$	1	2	7	19	Quase-Perfeito

Tabela 4.4: Perfeitos e quase-perfeitos para $p = 2$ e $n = 3$

Matriz Geradora	$\mathbf{r_p}$	$\mathbf{R_p}$	$\#\mathbf{B_p^n}(\mathbf{r_p})$	$\#\mathbf{B_p^n}(\mathbf{R_p})$	**Classificação**
$\begin{bmatrix} 1 & 1 & 2 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 4 \\ 0 & 0 & 13 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 3 \\ 0 & 0 & 13 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 5 \\ 0 & 0 & 13 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 5 \\ 0 & 0 & 13 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 6 \\ 0 & 0 & 13 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 6 \\ 0 & 0 & 13 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & 6 \\ 0 & 0 & 13 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 5 \\ 0 & 0 & 14 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 6 \\ 0 & 0 & 14 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 6 \\ 0 & 0 & 14 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & 6 \\ 0 & 0 & 14 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 5 \\ 0 & 0 & 15 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 5 \\ 0 & 0 & 15 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 6 \\ 0 & 0 & 15 \end{bmatrix}$	1	2	7	19	Quase-Perfeito

Tabela 4.5: Perfeitos e quase-perfeitos para $p = 2$ e $n = 3$ (continuação)

Matriz Geradora	$\mathbf{r_p}$	$\mathbf{R_p}$	$\#\mathbf{B_p^n(r_p)}$	$\#\mathbf{B_p^n(R_p)}$	**Classificação**
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 4 \\ 0 & 0 & 12 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 5 \\ 0 & 0 & 12 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 5 \\ 0 & 0 & 12 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 2 & 2 \\ 0 & 0 & 6 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 2 & 3 \\ 0 & 0 & 6 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 6 \\ 0 & 0 & 15 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & 6 \\ 0 & 0 & 15 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 7 \\ 0 & 0 & 15 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 7 \\ 0 & 0 & 15 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 3 & 0 \\ 0 & 0 & 5 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 1 & 2 \\ 0 & 3 & 0 \\ 0 & 0 & 5 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 6 \\ 0 & 0 & 16 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 6 \\ 0 & 0 & 17 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 6 \\ 0 & 0 & 17 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 8 \\ 0 & 0 & 17 \end{bmatrix}$	1	2	7	19	Quase-Perfeito

Tabela 4.6: Perfeitos e quase-perfeitos para $p = 2$ e $n = 3$ (continuação)

Matriz Geradora	$\mathbf{r_p}$	$\mathbf{R_p}$	$\#\mathbf{B_p^n(r_p)}$	$\#\mathbf{B_p^n(R_p)}$	**Classificação**
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 8 \\ 0 & 0 & 21 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 8 \\ 0 & 0 & 23 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 8 \\ 0 & 0 & 23 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 9 \\ 0 & 0 & 23 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 8 \\ 0 & 0 & 24 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 8 \\ 0 & 0 & 24 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 1 & 3 \\ 0 & 3 & 0 \\ 0 & 0 & 8 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 8 \\ 0 & 0 & 25 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 9 \\ 0 & 0 & 25 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 8 \\ 0 & 1 & 11 \\ 0 & 0 & 25 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 9 \\ 0 & 0 & 26 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 9 \\ 0 & 0 & 27 \end{bmatrix}$	3	3	27	27	Perfeito
$\begin{bmatrix} 1 & 0 & 6 \\ 0 & 1 & 9 \\ 0 & 0 & 27 \end{bmatrix}$	3	3	27	27	Perfeito
$\begin{bmatrix} 1 & 0 & 9 \\ 0 & 1 & 12 \\ 0 & 0 & 27 \end{bmatrix}$	3	3	27	27	Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 3 & 0 \\ 0 & 0 & 9 \end{bmatrix}$	3	3	27	27	Perfeito

Tabela 4.7: Perfeitos e quase-perfeitos para $p = 2$ e $n = 3$ (continuação)

Matriz Geradora	$\mathbf{r_p}$	$\mathbf{R_p}$	$\#\mathbf{B_p^n(r_p)}$	$\#\mathbf{B_p^n(R_p)}$	**Classificação**
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 3 & 3 \\ 0 & 0 & 9 \end{bmatrix}$	3	3	27	27	Perfeito
$\begin{bmatrix} 1 & 1 & 3 \\ 0 & 3 & 0 \\ 0 & 0 & 9 \end{bmatrix}$	3	3	27	27	Perfeito
$\begin{bmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix}$	3	3	27	27	Perfeito
$\begin{bmatrix} 1 & 0 & 11 \\ 0 & 1 & 16 \\ 0 & 0 & 35 \end{bmatrix}$	4	5	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 12 \\ 0 & 1 & 18 \\ 0 & 0 & 39 \end{bmatrix}$	4	5	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 13 \\ 0 & 0 & 41 \end{bmatrix}$	4	5	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 8 \\ 0 & 1 & 19 \\ 0 & 0 & 41 \end{bmatrix}$	4	5	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 13 \\ 0 & 1 & 19 \\ 0 & 0 & 41 \end{bmatrix}$	4	5	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 9 \\ 0 & 2 & 6 \\ 0 & 0 & 21 \end{bmatrix}$	4	5	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 4 \\ 0 & 3 & 7 \\ 0 & 0 & 14 \end{bmatrix}$	4	5	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 3 & 2 \\ 0 & 6 & 0 \\ 0 & 0 & 7 \end{bmatrix}$	4	5	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 14 \\ 0 & 1 & 20 \\ 0 & 0 & 44 \end{bmatrix}$	4	5	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 7 \\ 0 & 1 & 11 \\ 0 & 0 & 45 \end{bmatrix}$	4	5	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 8 \\ 0 & 1 & 13 \\ 0 & 0 & 45 \end{bmatrix}$	4	5	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & 17 \\ 0 & 0 & 45 \end{bmatrix}$	4	5	33	57	Quase-Perfeito

Tabela 4.8: Perfeitos e quase-perfeitos para $p = 2$ e $n = 3$ (continuação)

Matriz Geradora	$\mathbf{r_p}$	$\mathbf{R_p}$	$\#\mathbf{B_p^n}(\mathbf{r_p})$	$\#\mathbf{B_p^n}(\mathbf{R_p})$	**Classificação**
$\begin{bmatrix} 1 & 0 & 8 \\ 0 & 1 & 12 \\ 0 & 0 & 46 \end{bmatrix}$	4	5	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 13 \\ 0 & 0 & 47 \end{bmatrix}$	4	5	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & 18 \\ 0 & 0 & 47 \end{bmatrix}$	4	5	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 12 \\ 0 & 1 & 19 \\ 0 & 0 & 47 \end{bmatrix}$	4	5	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 8 \\ 0 & 1 & 12 \\ 0 & 0 & 50 \end{bmatrix}$	4	5	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 21 \\ 0 & 0 & 55 \end{bmatrix}$	4	5	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 25 \\ 0 & 0 & 63 \end{bmatrix}$	5	6	57	81	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 26 \\ 0 & 0 & 65 \end{bmatrix}$	5	6	57	81	Quase-Perfeito
$\begin{bmatrix} 1 & 1 & 5 \\ 0 & 5 & 0 \\ 0 & 0 & 13 \end{bmatrix}$	5	6	57	81	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 4 \\ 0 & 0 & 10 \end{bmatrix}$	8	9	93	123	Quase-Perfeito
$\begin{bmatrix} 1 & 1 & 5 \\ 0 & 6 & 6 \\ 0 & 0 & 18 \end{bmatrix}$	8	9	93	123	Quase-Perfeito

Tabela 4.9: Perfeitos e quase-perfeitos para $p = 2$ e $n = 3$ (continuação)

Matriz Geradora	$\mathbf{r_p}$	$\mathbf{R_p}$	$\#\mathbf{B_p^n(r_p)}$	$\#\mathbf{B_p^n(R_p)}$	**Classificação**
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 7 \end{bmatrix}$	1	1	7	7	Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 8 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 9 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 4 \\ 0 & 0 & 9 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 9 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 10 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 4 \\ 0 & 0 & 10 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 10 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 11 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 4 \\ 0 & 0 & 11 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 11 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 5 \\ 0 & 0 & 11 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 5 \\ 0 & 0 & 11 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & 5 \\ 0 & 0 & 11 \end{bmatrix}$	1	2	7	19	Quase-Perfeito

Tabela 4.10: Perfeitos e quase-perfeitos para $p = 3$ e $n = 3$

Matriz Geradora	$\mathbf{r_p}$	$\mathbf{R_p}$	$\#\mathbf{B_p^n}(\mathbf{r_p})$	$\#\mathbf{B_p^n}(\mathbf{R_p})$	**Classificação**
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 4 \\ 0 & 0 & 12 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 5 \\ 0 & 0 & 12 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 5 \\ 0 & 0 & 12 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 2 & 2 \\ 0 & 0 & 6 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 2 & 3 \\ 0 & 0 & 6 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 1 & 2 \\ 0 & 3 & 0 \\ 0 & 0 & 4 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 4 \\ 0 & 0 & 13 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 13 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 5 \\ 0 & 0 & 13 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 5 \\ 0 & 0 & 13 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 6 \\ 0 & 0 & 13 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 6 \\ 0 & 0 & 13 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & 6 \\ 0 & 0 & 13 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 5 \\ 0 & 0 & 14 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 6 \\ 0 & 0 & 14 \end{bmatrix}$	1	2	7	19	Quase-Perfeito

Tabela 4.11: Perfeitos e quase-perfeitos para $p = 3$ e $n = 3$ (continuação)

Matriz Geradora	$\mathbf{r_p}$	$\mathbf{R_p}$	$\#\mathbf{B_p^n}(\mathbf{r_p})$	$\#\mathbf{B_p^n}(\mathbf{R_p})$	**Classificação**
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 6 \\ 0 & 0 & 14 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & 6 \\ 0 & 0 & 14 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 5 \\ 0 & 0 & 15 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 5 \\ 0 & 0 & 15 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 6 \\ 0 & 0 & 15 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 6 \\ 0 & 0 & 15 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & 6 \\ 0 & 0 & 15 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 7 \\ 0 & 0 & 15 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 7 \\ 0 & 0 & 15 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 3 & 0 \\ 0 & 0 & 5 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 1 & 2 \\ 0 & 3 & 0 \\ 0 & 0 & 5 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 6 \\ 0 & 0 & 16 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 2 \\ 0 & 1 & 6 \\ 0 & 0 & 17 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 6 \\ 0 & 0 & 17 \end{bmatrix}$	1	2	7	19	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 8 \\ 0 & 0 & 17 \end{bmatrix}$	1	2	7	19	Quase-Perfeito

Tabela 4.12: Perfeitos e quase-perfeitos para $p = 3$ e $n = 3$ (continuação)

Matriz Geradora	$\mathbf{r_p}$	$\mathbf{R_p}$	$\#\mathbf{B_p^n(r_p)}$	$\#\mathbf{B_p^n(R_p)}$	**Classificação**
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 3 & 3 \\ 0 & 0 & 9 \end{bmatrix}$	3	3	27	27	Perfeito
$\begin{bmatrix} 1 & 1 & 3 \\ 0 & 3 & 0 \\ 0 & 0 & 9 \end{bmatrix}$	3	3	27	27	Perfeito
$\begin{bmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix}$	3	3	27	27	Perfeito
$\begin{bmatrix} 1 & 0 & 11 \\ 0 & 1 & 16 \\ 0 & 0 & 35 \end{bmatrix}$	8	9	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 12 \\ 0 & 1 & 18 \\ 0 & 0 & 39 \end{bmatrix}$	8	9	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 13 \\ 0 & 0 & 41 \end{bmatrix}$	8	9	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 8 \\ 0 & 1 & 19 \\ 0 & 0 & 41 \end{bmatrix}$	8	9	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 13 \\ 0 & 1 & 19 \\ 0 & 0 & 41 \end{bmatrix}$	8	9	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 9 \\ 0 & 2 & 6 \\ 0 & 0 & 21 \end{bmatrix}$	8	9	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 4 \\ 0 & 3 & 7 \\ 0 & 0 & 14 \end{bmatrix}$	8	9	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 3 & 2 \\ 0 & 6 & 0 \\ 0 & 0 & 7 \end{bmatrix}$	8	9	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 14 \\ 0 & 1 & 20 \\ 0 & 0 & 44 \end{bmatrix}$	8	9	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 7 \\ 0 & 1 & 11 \\ 0 & 0 & 45 \end{bmatrix}$	8	9	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 8 \\ 0 & 1 & 13 \\ 0 & 0 & 45 \end{bmatrix}$	8	9	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & 17 \\ 0 & 0 & 45 \end{bmatrix}$	8	9	33	57	Quase-Perfeito

Tabela 4.14: Perfeitos e quase-perfeitos para $p = 3$ e $n = 3$ (continuação)

Matriz Geradora	$\mathbf{r_p}$	$\mathbf{R_p}$	$\#\mathbf{B_p^n}(\mathbf{r_p})$	$\#\mathbf{B_p^n}(\mathbf{R_p})$	**Classificação**
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 8 \\ 0 & 0 & 21 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 8 \\ 0 & 0 & 23 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 8 \\ 0 & 0 & 23 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 9 \\ 0 & 0 & 23 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 8 \\ 0 & 0 & 24 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 8 \\ 0 & 0 & 24 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 1 & 3 \\ 0 & 3 & 0 \\ 0 & 0 & 8 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 8 \\ 0 & 0 & 25 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 9 \\ 0 & 0 & 25 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 8 \\ 0 & 1 & 11 \\ 0 & 0 & 25 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 9 \\ 0 & 0 & 26 \end{bmatrix}$	2	3	19	27	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 1 & 9 \\ 0 & 0 & 27 \end{bmatrix}$	3	3	27	27	Perfeito
$\begin{bmatrix} 1 & 0 & 6 \\ 0 & 1 & 9 \\ 0 & 0 & 27 \end{bmatrix}$	3	3	27	27	Perfeito
$\begin{bmatrix} 1 & 0 & 9 \\ 0 & 1 & 12 \\ 0 & 0 & 27 \end{bmatrix}$	3	3	27	27	Perfeito
$\begin{bmatrix} 1 & 0 & 3 \\ 0 & 3 & 0 \\ 0 & 0 & 9 \end{bmatrix}$	3	3	27	27	Perfeito

Tabela 4.13: Perfeitos e quase-perfeitos para $p = 3$ e $n = 3$ (continuação)

Matriz Geradora	$\mathbf{r_p}$	$\mathbf{R_p}$	$\#\mathbf{B_p^n(r_p)}$	$\#\mathbf{B_p^n(R_p)}$	**Classificação**
$\begin{bmatrix} 1 & 0 & 8 \\ 0 & 1 & 12 \\ 0 & 0 & 46 \end{bmatrix}$	8	9	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 13 \\ 0 & 0 & 47 \end{bmatrix}$	8	9	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & 18 \\ 0 & 0 & 47 \end{bmatrix}$	8	9	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 12 \\ 0 & 1 & 19 \\ 0 & 0 & 47 \end{bmatrix}$	8	9	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 8 \\ 0 & 1 & 12 \\ 0 & 0 & 50 \end{bmatrix}$	8	9	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 21 \\ 0 & 0 & 55 \end{bmatrix}$	8	9	33	57	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 25 \\ 0 & 0 & 63 \end{bmatrix}$	9	10	57	81	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 26 \\ 0 & 0 & 65 \end{bmatrix}$	9	10	57	81	Quase-Perfeito
$\begin{bmatrix} 1 & 1 & 5 \\ 0 & 5 & 0 \\ 0 & 0 & 13 \end{bmatrix}$	9	10	57	81	Quase-Perfeito
$\begin{bmatrix} 1 & 1 & 5 \\ 0 & 6 & 6 \\ 0 & 0 & 18 \end{bmatrix}$	16	17	93	117	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 25 \\ 0 & 0 & 123 \end{bmatrix}$	17	24	117	125	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 49 \\ 0 & 0 & 123 \end{bmatrix}$	17	24	117	125	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 49 \\ 0 & 1 & 59 \\ 0 & 0 & 123 \end{bmatrix}$	17	24	117	125	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 25 \\ 0 & 0 & 124 \end{bmatrix}$	17	24	117	125	Quase-Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 25 \\ 0 & 0 & 125 \end{bmatrix}$	24	24	125	125	Perfeito

Tabela 4.15: Perfeitos e quase-perfeitos para $p = 3$ e $n = 3$ (continuação)

Matriz Geradora	$\mathbf{r_p}$	$\mathbf{R_p}$	$\#\mathbf{B_p^n}(\mathbf{r_p})$	$\#\mathbf{B_p^n}(\mathbf{R_p})$	**Classificação**
$\begin{bmatrix} 1 & 0 & 10 \\ 0 & 1 & 25 \\ 0 & 0 & 125 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 15 \\ 0 & 1 & 25 \\ 0 & 0 & 125 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 20 \\ 0 & 1 & 25 \\ 0 & 0 & 125 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 25 \\ 0 & 1 & 30 \\ 0 & 0 & 125 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 25 \\ 0 & 1 & 35 \\ 0 & 0 & 125 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 25 \\ 0 & 1 & 40 \\ 0 & 0 & 125 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 25 \\ 0 & 1 & 45 \\ 0 & 0 & 125 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 1 & 50 \\ 0 & 0 & 125 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 10 \\ 0 & 1 & 50 \\ 0 & 0 & 125 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 15 \\ 0 & 1 & 50 \\ 0 & 0 & 125 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 20 \\ 0 & 1 & 50 \\ 0 & 0 & 125 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 30 \\ 0 & 1 & 50 \\ 0 & 0 & 125 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 35 \\ 0 & 1 & 50 \\ 0 & 0 & 125 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 40 \\ 0 & 1 & 50 \\ 0 & 0 & 125 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 45 \\ 0 & 1 & 50 \\ 0 & 0 & 125 \end{bmatrix}$	24	24	125	125	Perfeito

Tabela 4.16: Perfeitos e quase-perfeitos para $p = 3$ e $n = 3$ (continuação)

Matriz Geradora	$\mathbf{r_p}$	$\mathbf{R_p}$	$\#\mathbf{B_p^n}(\mathbf{r_p})$	$\#\mathbf{B_p^n}(\mathbf{R_p})$	**Classificação**
$\begin{bmatrix} 1 & 0 & 25 \\ 0 & 1 & 55 \\ 0 & 0 & 125 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 50 \\ 0 & 1 & 55 \\ 0 & 0 & 125 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 25 \\ 0 & 1 & 60 \\ 0 & 0 & 125 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 50 \\ 0 & 1 & 60 \\ 0 & 0 & 125 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 5 & 0 \\ 0 & 0 & 25 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 10 \\ 0 & 5 & 0 \\ 0 & 0 & 25 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 5 & 5 \\ 0 & 0 & 25 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 10 \\ 0 & 5 & 5 \\ 0 & 0 & 25 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 5 \\ 0 & 5 & 10 \\ 0 & 0 & 25 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 0 & 10 \\ 0 & 5 & 10 \\ 0 & 0 & 25 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 1 & 5 \\ 0 & 5 & 0 \\ 0 & 0 & 25 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 1 & 10 \\ 0 & 5 & 0 \\ 0 & 0 & 25 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 2 & 5 \\ 0 & 5 & 0 \\ 0 & 0 & 25 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 1 & 2 & 10 \\ 0 & 5 & 0 \\ 0 & 0 & 25 \end{bmatrix}$	24	24	125	125	Perfeito
$\begin{bmatrix} 5 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 5 \end{bmatrix}$	24	24	125	125	Perfeito

Tabela 4.17: Perfeitos e quase-perfeitos para $p = 3$ e $n = 3$ (continuação)

Referências Bibliográficas

[1] António Campello. *Reticulados, Projeções e Aplicações à Teoria da Informação*. PhD thesis, UNICAMP, 2014.

[2] António Campello. Notas de aula de tópicos em matemática aplicada, 2014.

[3] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices and groups*. 1999.

[4] U. Fincke and M. Pohst. Improved methods for calculating vectors of shorts length in a lattices, including a complexity analysis. *Mathematics of Computations*, 1985.

[5] Steven Galbraith. Mathematics of public key cryptography, 2012.

[6] Drielson D. S. Gouveia. Um estudo sobre o problema do vetor mais próximo nos reticulados raízes zn, an e dn: Algoritmos e simulações numéricas. Master's thesis, UNICAMP, 2011.

[7] A. Hefez and M. L. T. Vilella. *Códigos Corretores de Erros*. IMPA, 2002.

[8] P. Horak and B.F. Albdaiwi. Diameter perfect lee codes. *IEEE Transactions on Information Theory*, 2012.

[9] Grasiele Jorge, António Campello, and Sueli I. R. Costa. q-ary lattices in the lp norm and a generalization of the lee metric. In *q-ary Lattices in the lp Norm and a Generalization of the Lee Metric*, 2013.

[10] Ligia R. B. Naves. A densidade de empacotamentos esféricos em reticulados. Master's thesis, UNICAMP, 2009.

[11] Anderson Tiago da Silva. De códigos binários a reticulados e códigos esféricos. Master's thesis, UNICAMP, 2007.

[12] João E. Strapasson. *Geometria Discreta e Códigos*. PhD thesis, UNICAMP, 2007.

[13] João E. Strapasson, Grasiele Jorge, Antonio Campello, and Sueli I. R. Costa. Quasi - perfect codes in the lp metric. *ArXiv*, 2015.